FORTALECIMIENTO DEL ESQUEMA DE DEFENSA EN PROFUNDIDAD EN LA ANH PARA INCREMENTAR EL NIVEL DE PROTECCIÓN FRENTE A LAS AMENAZAS PERSISTENTES AVANZADAS.

DIEGO ALEJANDRO CARRILLO RICO

RAMIRO MERCHAN PATARROYO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
SEGURIDAD INFORMATICA
BOGOTÁ DISTRITO CAPITAL
2015

FORTALECIMIENTO DEL ESQUEMA DE DEFENSA EN PROFUNDIDAD EN LA ANH PARA INCREMENTAR EL NIVEL DE PROTECCIÓN FRENTE A LAS AMENAZAS PERSISTENTES AVANZADAS.

DIEGO ALEJANDRO CARRILLO RICO

RAMIRO MERCHAN PATARROYO

PROYECTO DE INVESTIGACIÓN

ALVARO ESCOBAR
DIRECTOR DE INVESTIGACIÓN

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
SEGURIDAD INFORMATICA
BOGOTÁ DISTRITO CAPITAL
2015

Nota de aceptación

_____
Firma del presidente

_____
Firma del jurado

_____
Firma del jurado

Bogotá Distrito Capital, 01/09/2015

CONTENIDO

pág.

TÍTULO **12**

INTRODUCCIÓN **13**

1. DEFINICIÓN DEL PROBLEMA **14**

2. JUSTIFICACIÓN **15**

3. OBJETIVOS **17**

3.1 OBJETIVO GENERAL 17
3.2 OBJETIVOS ESPECÍFICOS 17

4. MARCO REFERENCIAL **18**

4.1 PRESENTACIÓN DE LA ENTIDAD 18
4.2 MODELO DE DEFENSA EN PROFUNDIDAD 20
4.3 LAS AMENAZA AVANZADAS PERSISTENTES (APT´s) 24
4.3.1 Características de las APTs. *24*
4.3.2 Errores de Concepto en Relación con las APT. *25*
4.3.3 Proceso de Ataque. *25*
4.3.4 Métodos de Infección y Propagación. *26*

5. DISEÑO METODOLÓGICO **27**

5.1 TIPO DE INVESTIGACIÓN 27
5.2 FORMULACIÓN DE HIPOTESIS 27
5.3 DEFINICIÓN DE VARIABLES 27

6. RESULTADOS Y DISCUSIÓN **28**

6.1 EVALUACION DEL MODELO DE DEFENSA EN PROFUNDIDAD DE LA ANH 28
6.1.1 Propuesta de Evaluación de Arquitectura de Red Segura. *28*
6.2 RESULTADOS DIAGNÓSTICO DE SEGURIDAD 31
6.2.1 Protecciones Básicas de Red. *31*
6.2.2 Infraestructura de Enrutamiento. *34*
6.2.3 Recuperación y Supervivencia. *36*
6.2.4 Telemetría de Red. *36*
6.2.5 Aplicación de Políticas. *37*
6.2.6 Infraestructura de Switching. *38*
6.2.7 Mitigación de Amenazas a la Infraestructura. *39*
6.2.8 Frontera de Internet. *39*

6.2.9 Mitigación de Amenazas al Perímetro de Internet. 43
6.2.10 Frontera WAN. 43
Fuente: Autores 44
Fuente: Autores 45
6.2.11 Mitigación de Amenazas a la WAN. 45
6.2.12 Monitoreo, Análisis y Correlación. 45
6.3 RECOMENDACIONES 46
6.3.1 Recomendaciones asociadas a cumplimiento ISO/IEC 27002 47
6.3.2 Recomendaciones técnicas asociadas al cumplimiento mejores prácticas evaluadas. 49
6.4 ANÁLISIS DE VULNERABILIDADES TÉCNICAS 51
6.4.1 Hoja de Vida 52
6.4.2 Licenciamiento. 53
6.4.3 Actualizaciones. 53
6.4.4 Backups. 53
6.4.5 Funcionalidades por Activar. 53
6.4.6 Alertas Actuales. 53
6.4.7 Recomendaciones. 54
6.5 CONCLUSION 56
6.6 PLAN DE ACCION IMPLEMENTADO 56
6.6.1 Organización y plan de trabajo. 56
6.6.3 Resultados. 59
6.7 GESTIÓN DE VULNERABILIDADES TÉCNICAS 63
6.7.1 Análisis de vulnerabilidades de red. 63
6.7.2 Análisis de vulnerabilidades de aplicaciones. 64
6.7.3 Pruebas de Hacking Ético. 65
6.7.4 Gestión de Incidentes de seguridad informática. 66
6.7.5 Otras Acciones Emprendidas. 67
6.8 EVALUACION DE PRESENCIA DE APT´s EN LA ANH 70
6.8.1 Identificación de Herramientas de protección APT´s. 70
6.8.2 Comparación de las herramientas de protección APT. 74
6.8.3 Realización de Pruebas de Concepto (POC). 75
6.8.4 Análisis de Resultados. 78
6.8.5 Como Enfrentar las Amenazas Persistentes Avanzadas (APT´s). 79
6.8.6 Re-imaginando la seguridad. 85
6.8.7 Hay que Girar Hacia la Seguridad Adaptativa. 85
7. CONCLUSIONES 88
BIBLIOGRAFÍA 90

LISTA DE CUADROS

pág.

Cuadro 1. Escala de evaluación de riesgos **30**

Cuadro 2. Niveles de riesgo de acuerdo a la escala del cuadro tres **30**

Cuadro 3. Mejores prácticas e índice de riesgo para acceso lógico **33**

Cuadro 4. Mejores prácticas e índice de riesgo para enrutamiento **35**

Cuadro 5. Mejores prácticas e índice de riesgo para recuperación **36**

Cuadro 6. Mejores prácticas e índice de riesgo para telemetría **37**

Cuadro 7. Mejores prácticas e índice de riesgo para aplicación de políticas **38**

Cuadro 8. Mejores prácticas e índice de riesgo para switching **38**

Cuadro 9. Mitigación de amenazas a la infraestructura **39**

Cuadro 10. Mejores prácticas e índice de riesgo para frontera internet **41**

Cuadro 11. Mitigación de amenazas al perímetro de internet **44**

Cuadro 12. Amenazas claves en wan **44**

Cuadro 13. Mejores prácticas e índice de riesgo para frontera wan **45**

Cuadro 14. Mitigación de amenazas al perímetro de wan **46**

Cuadro 15. Mejores prácticas e índice de riesgo para monitoreo **47**

Cuadro 16. Recomendaciones de acuerdo a iso 27002 **47**

Cuadro 17. Recomendaciones de acuerdo mejores prácticas **49**

Cuadro 18. Programación de análisis de vulnerabilidades de aplicaciones **64**

Cuadro 19. Programación de análisis de vulnerabilidades de aplicaciones **74**

LISTA DE FIGURAS

pág.

Figura 1. Diagrama conceptual de funcionamiento de ti de la ANH **19**

figura 2. Crecimiento desordenado y heterogéneo de la infraestructura de TI **20**

figura 3. El modelo de defensa en profundidad **21**

figura 5. Conceptos de diseño y componentes del modelo de “defensa en profundidad **22**

figura 7. Esquema generalizado de protección perimetral en internet **40**

figura 8. Arquitectura de seguridad de red propuesta para la anh **52**

figura 9. Reporte inicial de vulnerabilidades técnicas **54**

figura 10. Reporte inicial de vulnerabilidades técnicas **54**

figura 11. Equipo de trabajo para la gestión y operación de ti, seguridad y drp **57**

figura 12. Diagrama de seguridad al cierre del proyecto **60**

figura 13. Evolución en la gestión de vulnerabilidades técnicas **65**

figura 14. Vulnerabilidades removidas **66**

figura 15. Porcentajes de remediación logrados **67**

figura 16. Ciclo de la arquitectura de seguridad adaptable **82**

figura 17. Uso de herramientas epp en las organizaciones **83**

figura 18. Recomendaciones de gartner group para fortalecer la seguridad **84**

figura 19. Seguridad convencional vs seguridad adaptativa **86**

GLOSARIO

ACCESOS NO AUTORIZADOS: acceso a un sistema mediante el uso ilegítimo de password u otro mecanismo, sin la autorización del propietario.[1]

APT: amenaza avanzada persistente. Es un adversario que posee sofisticados niveles de experiencia e importantes recursos, que le permiten crear oportunidades para lograr sus objetivos usando múltiples vectores de ataque (por ejemplo, con medios cibernéticos o físicos, y valiéndose de engaños).[2]

ÁREA: superficie continental o costa afuera comprendida dentro de uno o varios polígonos limitados en lo posible por líneas en dirección norte-sur y este-oeste, que determinan el o los Bloques del subsuelo en los cuales se otorgan los derechos a buscar hidrocarburos, a removerlos de su lecho natural, transportarlos hasta un punto en la superficie y adquirir la propiedad de la participación que corresponda al Contratista, en los términos del ordenamiento superior y del respectivo Contrato de Evaluación Técnica -TEA-, de Exploración y Producción -E&P- o Especial.[3]

ATAQUE MAN-IN-THE-MIDDLE (MITM): traducido al español “Hombre En Medio” u “Hombre en el medio”, se refiere a que existe alguien en medio de la comunicación entre el origen y el destino. El atacante puede observar, interceptar, modificar y retransmitir la información, dando origen a los siguientes posibles ataques posteriores.[4]

BOTNETS: conjunto de computadores infectados por malware que permite ejecutarlos de manera remota y trasparente al usuario, para dirigir ataques a objetivos con la finalidad de afectar la disponibilidad del servicio.

CONTRATOS ESPECIALES: contratos de exploración y explotación de hidrocarburos con características y/o estipulaciones particulares con respecto a los

[1] Stallings William; Computer Security, Principles and Practice, 3 Edition.
[2] National Institute Of Standars And Technology. NIST SP 800-63-1 Electronic authentication guideline
[3] Agencia Nacional de Hidrocarburos, www.anh.gov.co/mapa-de-tierras.aspx
[4] Stallings, Op. cit. p. 32

anteriores, que adopte el Consejo Directivo de la ANH, en función del desenvolvimiento tecnológico y/o el desarrollo del sector.[5]

CONTRATO DE EVALUACIÓN TÉCNICA (TEA): tiene como objeto otorgar al Contratista derecho exclusivo para realizar estudios de evaluación técnica en un área determinada, a sus únicos costo y riesgo y con arreglo a un programa específico, destinados a definir la prospectividad, a cambio del pago de unos derechos por concepto del uso del subsuelo y con el compromiso de entregar una participación en la producción y las demás retribuciones económicas aplicables.[6]

CONTRATO DE EXPLORACIÓN Y PRODUCCIÓN (E&P): tiene por objeto otorgar al Contratista derecho exclusivo para acometer y desarrollar actividades exploratorias en un área determinada y para producir los hidrocarburos propiedad del Estado que se descubran dentro de la misma, a sus únicos costo y riesgo y con arreglo a programas específicos, a cambio de retribuciones consistentes en el pago de regalías, derechos económicos y aportes a título de formación, fortalecimiento institucional y transferencia de tecnología.[7]

DEFENSA EN PROFUNDIDAD: filosofía que establece que: “los sistemas de seguridad de un sistema deben ser entendidos y contenidos dentro de capas, cada una independiente de la anterior de forma funcional y conceptual”.[8]

DENEGACIÓN DE SERVICIOS: (DOS): es un ataque a una red o a un sistema, que causa que un servicio o recurso sea inaccesible. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red víctima o sobrecarga de los recursos del sistema víctima.[9]

DENEGACIÓN DE SERVICIOS DISTRIBUIDO (DDoS): es un ataque de Denegación de servicios (DoS) realizado al mismo tiempo desde varios puntos, contra el mismo dispositivo de red.[10]

---

[5] Agencia Nacional de Hidrocarburos. Op. cit. Disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[6] Ibid., Disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[7] Ibid., Disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[8] ISACA. E-Commerce Security: Securing The Network Perimeter, 2004.
[9] Stallings, Op. cit. p. 33
[10] Ibid., Op. cit. p. 34

ESCALAMIENTO POR PRIVILEGIOS: ejecutar comandos desde una capa a nivel inferior con el fin de aumentar los privilegios de un usuario o apoderarse de otro.[11]

EXPLORACIÓN: la exploración es la primera actividad que deberá desarrollar el contratista a quien se le haya asignado un contrato de E&P en un determinado bloque y el fin principal es la búsqueda de estructuras favorables para la acumulación de hidrocarburos.[12]

EXPLOTACIÓN: comprende el desarrollo y la producción.[13]

LITOTECA: lugar físico destinado a la preservación de muestras de roca del subsuelo Colombiano, correspondientes a lugares geográficos donde se han desarrollado actividades de exploración o producción.[14]

PRUEBA DE CONCEPTO: PoC (por sus siglas en inglés) es una implementación parcial o incompleta de un método o de una idea, realizada con el propósito de verificar que el concepto o teoría en cuestión es susceptible de ser explotada de una manera útil. La PoC se considera habitualmente un paso importante en el proceso de crear un prototipo realmente operativo. En seguridad informática el término PoC se utiliza, a menudo, como sinónimo de Zero-Day Exploit. Esta es una vulnerabilidad que, por ser muy reciente, no aprovecha en su totalidad todas las ventajas que podría proporcionar. En este ámbito, la prueba de concepto se utiliza como demostración de que una aplicación o servicio puede ser vulnerable.[15]

RONDA: procedimiento competitivo de selección objetiva de contratistas. Puede ser un proceso abierto o cerrado. Este es parte del procedimiento de Asignación de Áreas para Exploración y Explotación.[16]

[11] Agencia Nacional de Hidrocarburos. Op. cit. Disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[12] Ibid., disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[13] Ibid., disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[14] Ibid., disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[15] Wikipedia. Disponible en internet: https://en.wikipedia.org
[16] Agencia Nacional de Hidrocarburos. Op. cit. Disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx

SESIONES HIJACKING: se refiere a la posibilidad de "duplicar" las credenciales de autorización en una comunicación válida ya establecida entre un server y un cliente para obtener el acceso a la información o los servicios en el server.[17]

YACIMIENTO: acumulación natural de hidrocarburos en el subsuelo.[18]

YACIMIENTO CONVENCIONAL: formación rocosa donde ocurren acumulaciones de hidrocarburos en trampas estratificadas y/o estructurales. Se caracteriza por un sistema natural de presión único, de manera que la producción de hidrocarburos de una parte del yacimiento afecta la presión de servorio en toda su extensión. Está limitado por barreras geológicas, tales como estratos impermeables, condiciones estructurales y agua en las formaciones y se encuentra efectivamente aislado de cualquier yacimiento que pueda estar presente en la misma área o estructura geológica.[19]

YACIMIENTO NO CONVENCIONAL: formación rocosa con baja permeabilidad primaria a la que se debe realizar estimulación para mejorar las condiciones de movilidad y recobro de hidrocarburos.[20]

[17] Stallings, Op. cit. p. 35
[18] Agencia Nacional de Hidrocarburos. Op. cit. Disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[19] Agencia Nacional de Hidrocarburos. Op. cit. Disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx
[20] Agencia Nacional de Hidrocarburos. Op. cit. Disponible en internet: www.anh.gov.co/mapa-de-tierras.aspx

RESUMEN

Este documento presenta el análisis y recomendaciones para fortalecer el modelo de defensa en profundidad de la Agencia Nacional de Hidrocarburos frente a las Amenazas Persistentes Avanzadas, trabajo realizado como requisito para optar al título de Especialista en Seguridad Informática de la Universidad Piloto de Colombia.

El proyecto pretende resolver la pregunta: ¿Qué elementos se deben incorporar o modificar en una arquitectura de seguridad para prevenir, detectar, contrarrestar y en general fortalecer la protección contra las APT en la ANH que ha basado su estrategia de protección en el modelo de defensa en profundidad?. Esta pregunta y en general el proyecto surgieron debido a que en la entidad se trabajó en el fortalecimiento de la estrategia protección de la información de manera consistente, basada en el modelo de defensa en profundidad, sin embargo se evidenció la presencia de vulnerabilidades ante las amenazas persistentes avanzadas.

Se realiza un recorrido por los conceptos de defensa en profundidad y amenazas persistentes avanzadas, incluyendo el diagnostico de red segura y de vulnerabilidades técnicas de la organización, generándose recomendaciones para fortalecer la arquitectura de red inicial. Así mismo integra la ejecución y resultados de una prueba de concepto sobre una herramienta de protección contra APT, las conclusiones sobre la eficiencia del modelo de seguridad y las recomendaciones para reducir aún más la posibilidad de éxito de este nuevo tipo de ataque, en función de una arquitectura de red mejorada frente a una arquitectura de seguridad adaptativa.

PALABRAS CLAVE: Defensa en profundidad, amenaza persistente avanzada, arquitectura de red segura, diagnostico de seguridad, prueba de concepto, análisis de vulnerabilidades técnicas, gestión de vulnerabilidades técnicas, herramientas de protección APT, seguridad adaptativa.

TÍTULO

FORTALECIMIENTO DEL ESQUEMA DE DEFENSA EN PROFUNDIDAD EN LA ANH PARA INCREMENTAR EL NIVEL DE PROTECCIÓN FRENTE A LAS AMENAZAS PERSISTENTES AVANZADAS.

INTRODUCCIÓN

La Agencia Nacional de Hidrocarburos (ANH) desde el año 2003 adquirió por parte del estado Colombiano la responsabilidad de administrar y regular el importante recurso hidrocarburifero de la nación con la finalidad de realizar una trasformación del sector de tal forma que se convirtiera en un negocio atractivo para los inversionistas nacionales y extranjeros. En cumplimiento de sus objetivos la organización implementa un modelo de contrato de regalías que divide las fases de exploración, evaluación y explotación manteniendo siempre el porcentaje de participación de la nación y siendo la dueña y administradora de la información que se desprenda de la ejecución de los contratos en cada una de sus fases.

Es así como la ANH tiene la responsabilidad de asegurar la valiosa información que administra y para ello ha implementado la estrategia de defensa en profundidad lo que le ha permitido ser una de las instituciones gubernamentales con la infraestructura más sólida del país, no obstante en el mundo actual ha surgido el concepto de amenazas persistentes avanzadas (APT) las que por sus características suponen un cambio en los esquemas actuales de la seguridad informática de las organizaciones.

El presente documento realiza un análisis del modelo de defensa en profundidad de la organización frente a las APT para determinar si es suficiente, puede adaptarse o definitivamente no es suficiente para protegerla ante las amenazas persistentes avanzadas.

1. DEFINICIÓN DEL PROBLEMA

¿Qué elementos se deben incorporar o modificar en una arquitectura de seguridad para prevenir, detectar, contrarrestar y en general fortalecer la protección contra las APT en una entidad de gobierno que ha basado su estrategia de protección en el modelo de defensa en profundidad?

2. JUSTIFICACIÓN

Los ataques contra la seguridad de la información y sus consecuencias en términos de pérdida de datos, perjuicios financieros, interrupción del servicio y daño de imagen no son una novedad. Los profesionales de seguridad enfrentan a diario amenazas como software malintencionado, la ingeniería social, la piratería informática, la inyección de código SQL y la denegación de servicios, que se han convertido en vectores de ataque convencionales. La postura frente a los mismos se concentra en la implementación de controles preventivos y detectivos para obstaculizar el trabajo de los atacantes (Defensa en profundidad). Vencer dichos controles sólo es cuestión de tiempo.

Los recientes ataques a gran escala contra la seguridad sacaron a la luz pública una nueva clase de amenaza para las redes: Las APT. Estas amenazas, vistas hasta ahora, como actividades patrocinadas por estados-gobiernos y dirigidas a redes gubernamentales, pasaron a ser un serio problema para las empresas, sino, pidamos la opinión a RSA, Google y la misma Nasa.

Existen diferencias apreciables entre las APT y las amenazas tradicionales, aunque las primeras aprovechan mucho de los vectores de ataque conocidos, sin embargo, existen diferentes y variadas opiniones en el mercado sobre lo que es una APT. Por lo general, las APT tienen por objetivo robar propiedad intelectual (espionaje) antes que obtener una ganancia financiera inmediata. Para efectos del presente anteproyecto se toma como entrada la definición del Instituto Nacional de Normas y Tecnología de los E.E.U.U. (NIST):

> Un APT es un adversario que posee sofisticados niveles de experiencia e importantes recursos, que le permiten crear oportunidades para lograr sus objetivos usando múltiples vectores de ataque (por ejemplo, con medios cibernéticos o físicos, y valiéndose de engaños). Generalmente, estos objetivos abarcan el establecimiento y la extensión de puntos de apoyo dentro de la infraestructura de tecnología de la información de las organizaciones a las que está dirigido el ataque, con el fin de extraer información, socavar u obstaculizar aspectos decisivos de una misión, un programa o una organización; o colocarse en una posición que le permita concretar estos objetivos en un futuro. La amenaza persistente avanzada: (i) procura lograr sus objetivos reiteradamente durante un periodo prolongado; (ii) se adapta a los esfuerzos realizados para defenderse y resistir el ataque; y (iii) está preparada para mantener el nivel de interacción que le permitirá concretar sus objetivos[21]

En 2013 y 2014, ISACA realizó una encuesta a nivel mundial indagando el conocimiento y postura de los profesionales de seguridad frente a las APT. Como principales conclusiones se obtuvieron la heterogeneidad de concepciones, el sub-dimensionamiento de este tipo de amenazas y el enfoque de defensa como si fuesen ataques convencionales.

[1] National Institute of Standards and Technology (NIST), Special publication 800-39, Managing information security risk, organization, misión and information systems, EEUU 2011

Se considera que la definición del NIST requiere mayor desglose en nuestro medio y por ello el proyecto a realizar ataca estas situaciones particulares en una entidad de gobierno que se ha propuesto como meta para 2015 fortalecer el esquema de defensa actual incluyendo la protección contra APT, lo cual redundara en la mitigación de riesgos y mejor tratamiento de los incidentes de seguridad que se presenten.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer los elementos claves en la definición de un plan de trabajo para fortalecer el esquema de protección contra las APT en la ANH, quien basa su seguridad en el modelo de defensa en profundidad.

3.2 OBJETIVOS ESPECÍFICOS

- Comprender el modelo de defensa en profundidad (Defense in Depth).
- Comprender el concepto de amenaza persistente avanzada.
- Evaluar el modelo de defensa en profundidad existente en la ANH y los ajustes requeridos al mismo para fortalecer la protección contra APT.
- Establecer el papel que juega cada uno de los elementos del modelo de defensa en profundidad en un esquema de protección contra APT.
- Definir el procedimiento administrativo, técnico y operativo para detectar la presencia de APT en la infraestructura de la organización.
- Identificar las características claves de las herramientas de protección contra APT y su integración con el modelo de defensa en profundidad.
- Formular el plan de trabajo para la definición e implementación de un esquema de protección contra APT integrado al modelo de defensa en profundidad.

4. MARCO REFERENCIAL

4.1 PRESENTACIÓN DE LA ENTIDAD

Con el Decreto 1760 de 2003 se consolidó la reestructuración del sector hidrocarburífero colombiano con la creación de la Agencia Nacional de Hidrocarburos como respuesta a la situación crítica que atravesaba Colombia debido a la disminución de las reservas de petróleo, lo cual eventualmente, llevaría al país a convertirse en importador de crudo.

De esta forma, la Agencia Nacional de Hidrocarburos adquirió de Ecopetrol su labor de administrador y regulador del recurso hidrocarburífero de la nación, y comenzó la transformación de Colombia en un país nuevamente prospectivo y atractivo para los inversionistas nacionales y extranjeros. Sin embargo, Ecopetrol mantiene todas las áreas que tenía bajo operación directa y los contratos de Asociación firmados hasta diciembre 31 de 2003.

Otro cambio fundamental fue la adopción del nuevo contrato de regalías, impuestos y derechos, que reemplazó el contrato de asociación. Este modelo contempla tres (3) etapas diferentes y separadas: exploración, evaluación y explotación, cuya duración está alineada con los estándares internacionales y genera una participación para el Estado entre el 50 y 60%.

Los términos económicos de la nueva forma de contrato convierten a Colombia en uno de los países más atractivos del mundo tanto en participación gubernamental como en utilidades de los inversionistas; y las áreas se asignan mediante procedimientos modernos, transparentes y eficientes a través de mecanismos adecuados de administración y seguimiento lo que garantiza procesos con altos estándares internacionales.

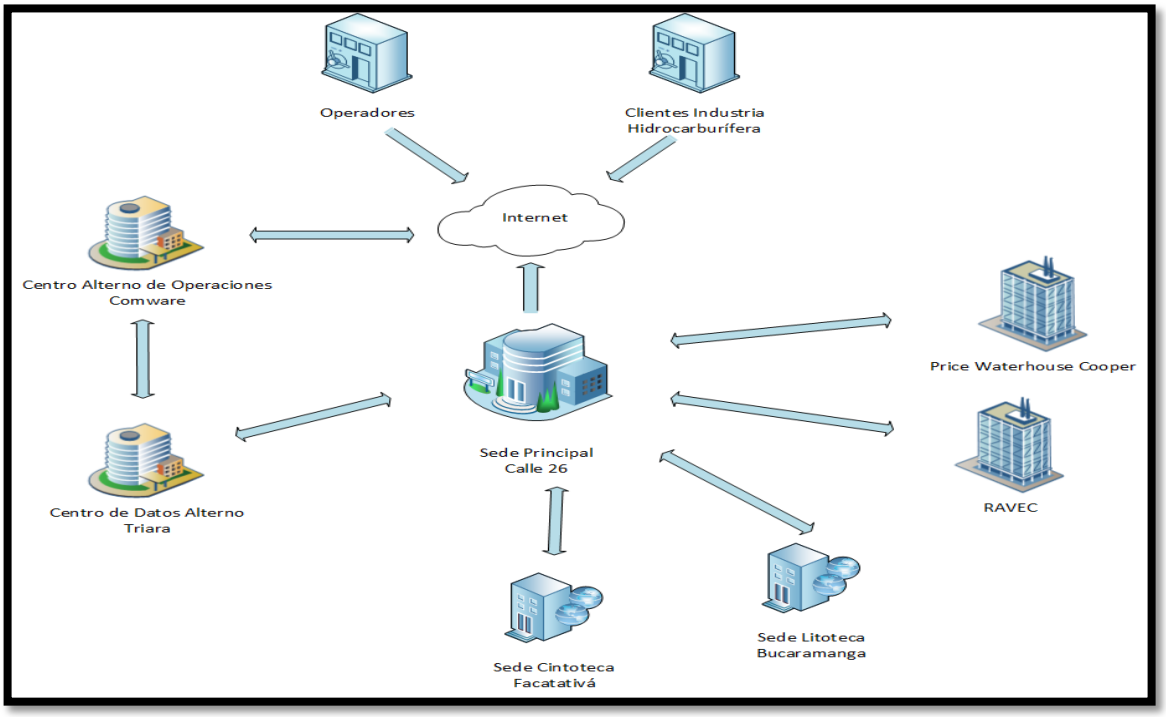
Igualmente, el modelo es conveniente para proyectos y compañías grandes, así como para pequeñas y medianas empresas abriendo un gran abanico de oportunidades para todos los inversionistas. Por otro lado, se introdujo el contrato de evaluación técnica (TEA) mediante el cual se puede asignar un área de gran tamaño para realizar trabajos de superficie con el fin de obtener mejor información sobre la presencia de hidrocarburos en una zona específica, y el cual puede tener una duración de hasta 18 meses. El contratista de un TEA cuenta con la primera opción para firmar un contrato de exploración y producción en esa área.

Para la asignación de áreas de exploración y producción se ideo el mecanismo de Rondas, en las cuales la ANH expone al mundo el potencial hidrocarburifero en diferentes áreas geográficas del país y los inversionistas concursan por la asignación de las mismas con base en los estudios existentes, la consulta a la litoteca y resultados de exploraciones anteriores.

El diagrama conceptual de funcionamiento de tecnología de la información de la entidad se aprecia a continuación. Ver figura 1. Sobre este diagrama se realizaron las siguientes evaluaciones e intervenciones:

- Inventario de activos de información
- Matriz de riesgos de TI
- Análisis de vulnerabilidades
- Evaluación del modelo de red ideal segura
- Fortalecimiento de la seguridad perimetral
- Definición de políticas de seguridad de la información
- Aseguramiento de servidores y dispositivos de comunicaciones
- Evaluación (pruebas de concepto) de presencia de APT´s

Figura 1. Diagrama conceptual de funcionamiento de TI de la ANH



Fuente: Contrato ANH 121 DE 2014

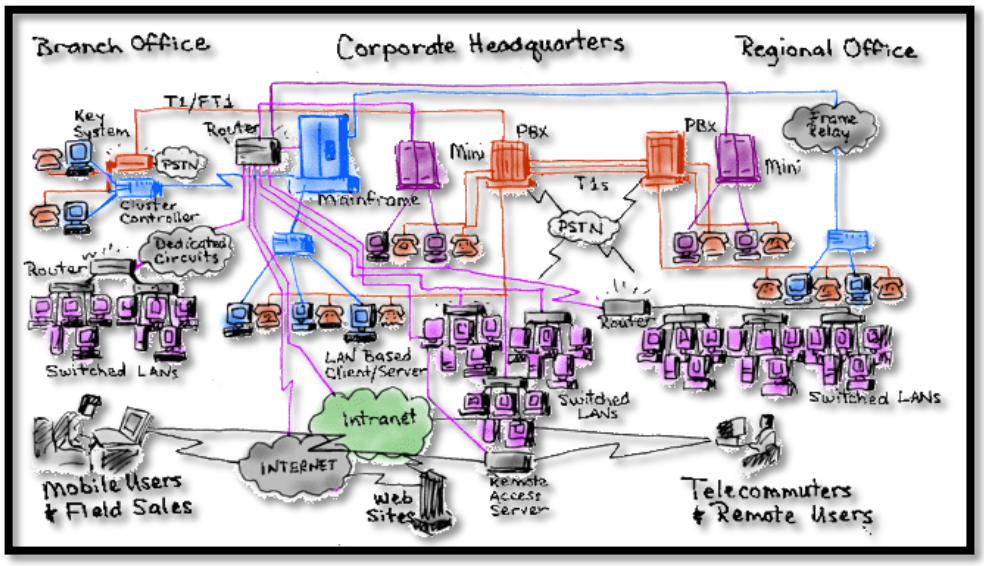
4.2 MODELO DE DEFENSA EN PROFUNDIDAD

La promesa de servicio de toda empresa o entidad se puede resumir en una frase**: "A cualquier hora desde cualquier lugar"**. Para cumplirla, las compañías trabajan fuertemente en la aplicación de los principios de la computación distribuida: Interconectividad e interoperabilidad, lo cual ha derivado en una gran demanda de infraestructura y que en la mayoría de los casos se implementa de manera desordenada.

El crecimiento desordenado y heterogéneo de la infraestructura de TI trae consigo, entre otras, las siguientes implicaciones:

- Rigidez y poca agilidad para que la tecnología gire hacia las necesidades empresariales.
- Mayor infraestructura significa mayores costos, procesos y personas.
- Más procesos implican mayores niveles de vulnerabilidad. Sobre una infraestructura compleja se dificulta cumplir con regulaciones y requerimientos de seguridad.
- Asegurar la información, su disponibilidad e integridad 7x24 es más complejo.
- No es claro donde inicia y donde termina el perímetro.

Figura 2. Crecimiento desordenado y heterogéneo de la infraestructura de TI



Fuente: Digiware. Information security trends 2010

Sobre este panorama tecnológico las organizaciones enfrentan el reto de implementar la seguridad de la información.

La filosofía Defensa en Profundidad - “Defense in Depth”, establece que: “los sistemas de seguridad de un sistema deben ser entendidos y contenidos dentro de capas, cada una independiente de la anterior de forma funcional y conceptual”. Ver figura 3.

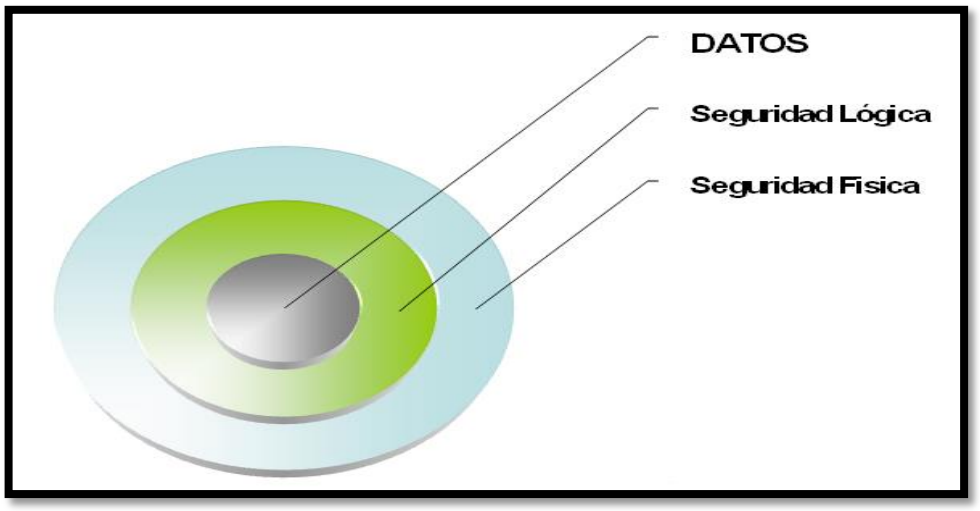
El modelo recomienda no olvidar los siguientes postulados:

- Si todo lo que se encuentra entre su información más sensitiva y un atacante es una sola capa de seguridad, el trabajo del atacante se hace sencillo.

- Ninguna medida de seguridad; y en un concepto más amplio, ninguna capa de seguridad, es infalible contra los ataques.

- Al agregar capas independientes a la arquitectura de seguridad se aumenta el tiempo que puede tomar el atacar un sitio, lo que permitiría en últimas detectar las intrusiones y los ataques justo cuando estos ocurren.

Figura 3.El modelo de defensa en profundidad

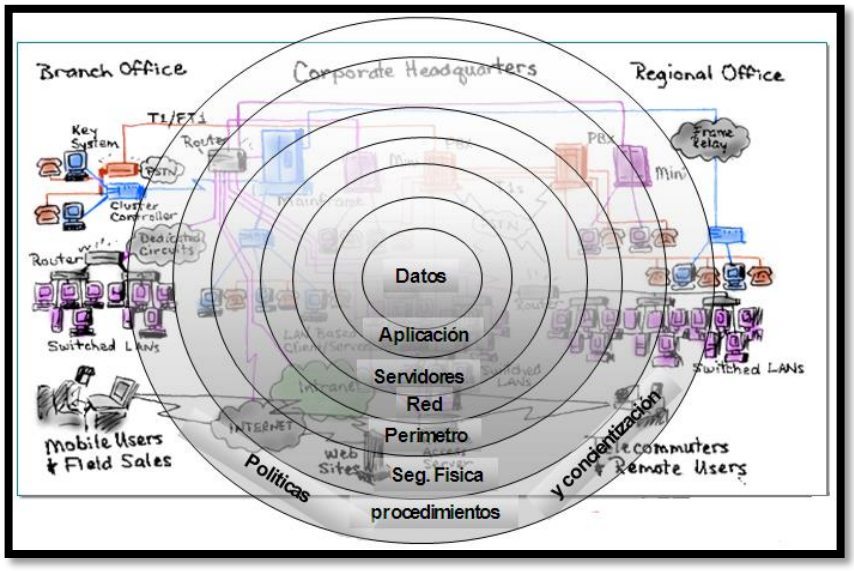


Fuente: ISACA – E-Commerce Security.Securing The Network Perimeter, 2004

Sumando las implicaciones de una infraestructura compleja junto con el concepto de defensa en profundidad, el reto o la pregunta que enfrenta toda organización es:

¿Es posible la implementación de medidas de seguridad efectivas sobre una infraestructura tecnológica compleja? Ver figura 4.

Figura 4. Vista conceptual para implementar seguridad sobre infraestructuras complejas de T.I.



Fuente: Digiware. Information security trends, 2010

El qué hacer lo propone el mismo modelo de Defensa en Profundidad: Es necesario diseñar el concepto de defensa en profundidad en la organización e implementar en consecuencia los componentes de tecnología requeridos. Ver figura 5.

Figura 5.Conceptos de diseño y componentes del modelo de "Defensa en Profundidad

CONCEPTOS DE DISEÑO

- EVALUACIÓN DE RIESGOS
- ESTRATEGIAS Y ESTÁNDARES
- ZONAS SEGURAS
- ENDURECIMIENTO DE SISTEMAS
  - Endurecimiento del Sistema Operacional
  - Eliminar servicios no requeridos
  - Actualización periódica de parches (sistemas operativos y aplicaciones)
  - Desactivar protocolos no encriptados
  - Protección contra virus
  - Renombrar cuentas de administrador
  - Cambiar passwords por defecto
  - Desactivar cuentas de invitado
  - No permitir anonimus FTP
  - Incrementar tamaño de archivos de log
  - Permisos sobre directorios, archivos y otros objetos
  - Desplegar mensajes de alerta
  - Implementar el concepto de menor privilegio
  - Separación de funciones

COMPONENTES

- ENRUTADORES
- SWITCHES
- FIREWALLS
- ACCESO REMOTO – VPN
- ACCESO REMOTO – DIAL UP
- REDES INALAMBRICAS
- DETECCIÓN DE INTRUSIONES
- EVALUACION DE LA SEGURIDAD DE LA RED
  - Análisis de vulnerabilidades

Fuente**:** ISACA.E-Commerce Security: securing the network perimeter, 2004

Las organizaciones invierten normalmente en los componentes y descuidan la columna de conceptos de diseño, lo que conlleva a que el retorno de la inversión

en seguridad se cuestione de manera permanente debido a la frecuencia de incidentes: Virus, fuga de información, interrupciones, ataques informáticos, fraudes entre otros.

El concepto de diseño del modelo exige que la organización trabaje sobre cuatro (4) aspectos:

Evaluación de riesgos: En el cual se debe establecer el perfil de riesgo de la organización, identificar las vulnerabilidades potenciales, incluyendo su probabilidad e impacto y los riesgos que genera: Pérdida de imagen y reputación, afectación de la privacidad, integridad de la información y no disponibilidad de los procesos del negocio, principalmente.

Estrategias y estándares: Es necesario que la organización defina e implemente procedimientos, estrategias y estándares que le brinden protección sobre los riesgos identificados. En este punto es importante que la organización trabaje en la definición e implementación de un sistema de gestión de la seguridad de la información – SGSI.

Endurecimiento de sistemas: Es necesario que en la organización se implementen y mantengan "Sistemas Robustos", lo cual significa trabajar en tres frentes:

- Fortalecimiento del sistema operacional.
- Implementación del concepto del menor privilegio.
- Segregación de funciones.

Zonas seguras: Al interior de la red de una organización es necesario implementar zonas de seguridad en las cuales sea posible aislar la información de acuerdo a la sensibilidad de la misma. Es necesario que la red de su empresa cuente con las siguientes zonas de seguridad:

- Insegura: Requiere autenticación de acceso para recursos específicos de información de los sistemas expuestos y accesibles públicamente.
- Semi-segura: Requieren autenticación de acceso para proteger los sistemas expuestos y no accesibles públicamente: Soporte a vendedores, socios de negocios
- Segura: Sistemas bajo el control directo de la Organización. Los usuarios requieren acceso total a los sistemas internos.
- Hostil: Acceso restringido sólo a los sistemas requeridos; los accesos no autorizados deben detectarse en tiempo real.

4.3 LAS AMENAZA AVANZADAS PERSISTENTES (APT´s)

El termino Amenazas Persistentes Avanzadas (APTs) se ha posicionado en la industria de la seguridad tanto de empresas de los sectores privado como Gubernamentales, para identificar los tipos de riesgos de ciberseguridad que por sus características pueden generar impactos mayores que las amenazas actuales.

Entre los principales rasgos de las APT se tienen:

- La capacidad de perdurar en el tiempo.
- La capacidad para aprovecharse de vulnerabilidades oficialmente desconocidas.
- El estar dirigidas a objetivos específicos.

Aunque en definitiva las APT tratan de comprometer una red de computadores para conseguir información sensible, se ha posicionado como principal objetivo de las APT el espionaje empresarial, gubernamental y militar, obteniendo y manipulando información contenida en los sistemas de la organización atacada, sin concentrase específicamente en atacar objetivos físicos .

4.3.1 Características de las APTs. Las Amenazas Persistentes Avanzadas suelen manifestarse como un programa especialmente diseñado para mantenerse oculto en el sistema atacado, puede que aprovechando vulnerabilidades desconocidas hasta ese momento, o usando técnicas de ingeniería social muy concretas sobre el personal de la empresa víctima. Esto quiere decir que se aleja del malware o amenazas comunes, que por lo general, son impersonales y generalistas.

El tipo de atacante que usa una APT es mucho más paciente que el atacante medio sin objetivo concreto. Suelen tener una mayor motivación económica para que el ataque sea exitoso y, por tanto, los recursos y tiempo empleados son superiores a los de cualquier otro atacante, lo cual lo ha convertido en un tipo de servicio demandado por competidores empresariales, caza-recompensas, gobiernos, servicios de inteligencia, etc.

Una característica habitualmente desarrollada en este tipo de amenazas es su capacidad de fragmentación o descomposición en módulos. Una vez infectado el sistema, este puede descargar módulos encargados de diferentes tareas, tales como leer comunicaciones de red, escuchar el micrófono e incluso controlar la webcam, sin que aparentemente estén relacionados.

4.3.2 Errores de Concepto en Relación con las APT. Hoy en día es frecuente la utilización del término APT para denominar ataques a organizaciones, gobiernos o empresas. Se han dado casos de malas interpretaciones, confundiendo verdaderos ataques dirigidos con errores y malas prácticas en el aseguramiento de un entorno empresarial. En este sentido, si no se establece de manera adecuada el nivel de riesgos en seguridad de la organización, un descuido, una mala gestión o una falta de previsión puede terminar en el compromiso de un sistema. Por ello, no siempre se debe poner este problema como excusa y culpar del hecho a ataques invisibles APTs, por ejemplo, que un empleado haya abierto un correo infectado y la red de la empresa haya quedado comprometida.

Del mismo modo, no se debe caer en el error de pensar que siempre que una compañía importante sufre una intrusión ha sido víctima de una APT. Tampoco hay que dar por hecho que cuando organizaciones de menor calibre son quienes los sufren, es por una falta de seguridad.

Si se toma como válido el concepto de APTs se deben identificar:

- Amenaza: ¿Es realmente una amenaza? Se deberían considerar como tales aquellos que persiguen un objetivo concreto e importante (espionaje industrial, cuentas bancarias, bloqueo de infraestructuras civiles o militares, etc.). Se trata, por tanto, de objetivos de cierta envergadura.

- Persistente: ¿Se trata realmente un ataque persistente? Es necesario matizar esto. El que un ataque se prolongue en el tiempo no debería ser factor tan determinante. Existen sitios web que sufren intentos de denegación de servicio durante días o semanas y también ataques que se han llevado con precisión milimétrica, bien porque se conocía de antemano la infraestructura de la empresa (un caso de estudio previo) o porque se tenía localizada una vulnerabilidad que permitía una rápida explotación sin tener que llevar a cabo intentos posteriores para acceder a la información u objetivo del ataque. En cualquiera de los dos casos, se requiere un trabajo previo. Por tanto, la persistencia no radica en la duración del ataque sino en el tiempo empleado para su ejecución.

- Avanzada: ¿Consiste realmente en un ataque avanzado? Debe aportar alguna novedad en el campo de la seguridad y ser específico para el objetivo atacado.

4.3.3 Proceso de Ataque. El proceso general por parte de los atacantes consta de varias partes:

- Estudio de la víctima: Al tratarse de un ataque específico dirigido, el atacante debe conocer en profundidad su objetivo, desde la configuración de los

sistemas hasta sus políticas de seguridad. Esto le permite elegir el punto más débil en la cadena para atacar.

- Infección: Consiste en instalarse o esconderse en alguna máquina de la red interna, desde donde se intenta obtener el objetivo deseado (la información). Esta máquina puede infectarse ejecutando un simple archivo, que contiene las instrucciones para futuras etapas de la infección. También incluye la lógica necesaria para descargar nuevas funcionalidades, si fuesen necesarias.

- Propagación: Una vez infectado un equipo o sistema, la propagación consiste en extenderse a más equipos, ya sean en la red colindante (LAN) o a través de Internet. Con esto se consigue más información. Como contrapartida, el atacante asume un mayor riesgo a ser detectado.

4.3.4 Métodos de Infección y Propagación. A continuación se enumeran distintos métodos que, aprovechados de una manera u otra, pueden servir para infectar sistemas o para propagar el malware:

- Ingeniería social.

- Incremento de las exposiciones por la masificación de dispositivos móviles de propiedad de los usuarios (BYOD).

- Vulnerabilidades presentes en la infraestructura.

- Phishing dirigido.

- Debilidades en las defensas perimetrales.

- Distracciones (ataques señuelo).

5. DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

Gestión de la seguridad y el riesgo.

5.2 FORMULACIÓN DE HIPOTESIS

H1: El modelo en Defensa en profundidad de la empresa ABC se fortalecerá mediante la aplicación de estrategias o mecanismos de control para detectar la presencia, prevenir o reaccionar a ataques tipo APT.

H0: En la empresa ABC no es posible fortalecer el modelo de defensa en profundidad mediante la aplicación de estrategias o mecanismos de control para prevenir y reaccionar a ataques tipo APT.

5.3 DEFINICIÓN DE VARIABLES

Variables dependientes

- APT
- Modelo de defensa en profundidad
- Estrategias o mecanismos de control

Variables independientes

- Ataques tipo APT

6. RESULTADOS Y DISCUSIÓN

6.1 EVALUACION DEL MODELO DE DEFENSA EN PROFUNDIDAD DE LA ANH

Si bien en el ejercicio realizado, durante un lapso de 2 años, se llevaron a cabo evaluaciones de riesgos de TI, pruebas de ingeniería social, evaluación de la seguridad física de los centros de cómputo, entre otras, en el presente estudio se profundizo en dos actividades centrales para los objetivos propuestos:

- Evaluación de la seguridad de red bajo el modelo de defensa en profundidad y
- Análisis de vulnerabilidades técnicas.

Los reportes iniciales de evaluación de red segura y análisis de vulnerabilidades técnicas se describen a continuación:

6.1.1 Propuesta de Evaluación de Arquitectura de Red Segura.

La constante evolución del mundo de la seguridad lleva a las organizaciones a un continuo cambio. La rápida proliferación de bootnets, el incremento sofisticado de ataques de red, el amplio crecimiento de crímenes y espionaje basados en Internet, el robo de identidad y datos, y nuevas formas de ataques sobre los sistemas, son ejemplos de los diversos ataques a los que el mundo de la seguridad se está enfrentando.

Como un factor clave de la actividad empresarial, las redes deben ser diseñadas e implementadas teniendo en mente la seguridad, para así asegurar la confidencialidad, integridad y disponibilidad de los datos y recursos que soportan las funciones claves del negocio. En esta sección se presenta la evaluación con base en las buenas prácticas de acuerdo con estándares internacionales, como NIST y SANS y fabricantes como CISCO, Check Point, entre otros; del diseño y configuración de la seguridad implementada por la Agencia Nacional de Hidrocarburos - ANH.

Lograr el nivel adecuado de seguridad, depende de la interrelación de todos los elementos, no solo dispositivos de seguridad como firewalls, IPS, Antivirus, sino de la unión de éstos con los dispositivos de Networking y Switching. Es por esto que el diagnóstico de seguridad adopta un enfoque en defensa en profundidad, donde múltiples capas de protección son estratégicamente configuradas. En general, el diseño e implementación de una Arquitectura de red Segura debe estar basada en los principios de defensa en profundidad, modularidad y flexibilidad,

disponibilidad y capacidad de recuperación, cumplimiento de regulaciones, e implementaciones auditables.

6.1.2 Metodología de Evaluación de Arquitectura de Red Segura. Dentro del desarrollo de una Arquitectura es necesario tener en cuenta dos aspectos claves:

- Arquitectura Funcional: la cual describe los tipos de datos que necesitan ser procesados y transmitidos, así como el ancho de banda necesario y el tipo de topología a usar (hub and spoke, Star, Ethernet, Token Ring y demás).

- Arquitectura Física: Desarrollada para complementar y soportar la arquitectura funcional.

La Arquitectura debe proporcionar mecanismos de seguridad mediante la implementación de los niveles apropiados para incrementar la confidencialidad, integridad, disponibilidad y medición del Sistema.

De acuerdo al Information Systems Security Architecture Profesional (ISSAP), una Arquitectura de Seguridad incluye, el hardware, el software, los procesos y el ambiente como parte del conjunto de los sistemas de Información y Seguridad. Una de las mejores prácticas dentro de una Arquitectura es el manejo de Defensa en Profundidad, en donde capas de tecnología son diseñadas e implementadas para proporcionar la protección a los datos. La base de la Defensa en Profundidad se concentra en:

- Proteger – controles y mecanismos preventivos

- Detectar – Identificar ataques, esperar ataque.

- Reaccionar – Responder ante ataques, recuperarse

Los requerimientos de seguridad varían dependiendo del tipo de negocio o compañía. Por ejemplo, parte de la industria de la salud en Estados Unidos debe cumplir con el HIPPA. Otras organizaciones que manejan personal y privacidad de datos deben cumplir los requisitos de Sarbanes-OxleyAct del 2002; de igual forma organizaciones que procesan información de tarjetas de crédito deben cumplir con PCI DSS; y en Europa con la Directiva 95/46/EC y la Directiva 2002/58/EC se pretende dar cumplimiento a la Protección de los Datos y la Privacidad. Sin embargo existen ciertos estándares que incluyen organizaciones de todo tipo como lo es la ISO/IEC 27001:2013, ésta especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener, y mejorar un Sistema de Gestión de Seguridad de la Información documentado dentro del contexto del riesgo dentro de la organización.

Para el caso de ANH, el diagnóstico de seguridad perimetral se realizó basado en las mejores prácticas de Defensa en Profundidad vs Nivel de Riesgo. Dentro de cada uno de los ítems a evaluar, se le otorgó una calificación de nivel de riesgo basado en su probabilidad y severidad.

La escala de evaluación utilizada se presenta en el siguiente cuadro:

Cuadro 1. Escala de evaluación de riesgos

Probabilidad de riesgo	Severidad del riesgo				
	Catastrófico A	Crítico B	Moderado C	Menor D	Despreciable E
5 – Frecuente	5A	5B	5C	5D	5E
4 – Probable	4A	4B	4C	4D	4E
3 – Ocasional	3A	3B	3C	3D	3E
2 – Raramente	2A	2B	2C	2D	2E
1 – Improbable	1A	1B	1C	1D	1E

Fuente: Cisco SAFE Reference Guide. Cisco Validated Design. July 8, 2010

La interpretación del nivel de riesgo se realiza con base en el siguiente cuadro:

Cuadro 2. Niveles de Riesgo de acuerdo a la escala del cuadro tres

Nivel de riesgo	Índice de valoración del riesgo	Criterio
4	5A, 5B, 5C, 4A, 4B, 3ª	Inaceptable bajo condiciones actuales. Requiere acción inmediata
3	5D, 5E, 4C, 3B, 3C, 2A, 2B	Manejable bajo una mitigación y control del riesgo. Requiere una decisión por parte de RAB[22] y administración.
2	4D, 4E, 3D, 2C, 1A, 1B	Aceptable después de revisar la operación. Requiere monitoreo continuo y planes de acción documentados.
1	3E, 2D, 2E, 1C, 1D, 1E	Aceptable con permanente recolección de datos y tendencias de mejora continua.

Fuente: Cisco SAFE Reference Guide. Cisco ValidatedDesign. July 8, 2010

Una vez identificados los niveles de riesgos se generaron las recomendaciones basadas en:

- Controles Perimetrales para ISO 27000, tipo procedimental.

[22] RAB Risk Analysis Board – Equipo de Análisis de Riesgos

- Controles técnicos, con su correspondiente justificación. Para dar mayor énfasis, serán justificados los que se encuentren en los índices DE COLOR ROJO (5A, 5B, 5C, 4A, 4B, 3A).

6.2 RESULTADOS DIAGNÓSTICO DE SEGURIDAD

Existen recomendaciones de diseño para ampliar el nivel de seguridad de una infraestructura de red y guías de mejores prácticas para generar planes de control y administración de dicha infraestructura. Cada una de estas áreas se analizó dentro de la infraestructura de red de la compañía, para el caso de ANH, se analizaron los siguientes módulos dentro de su infraestructura:

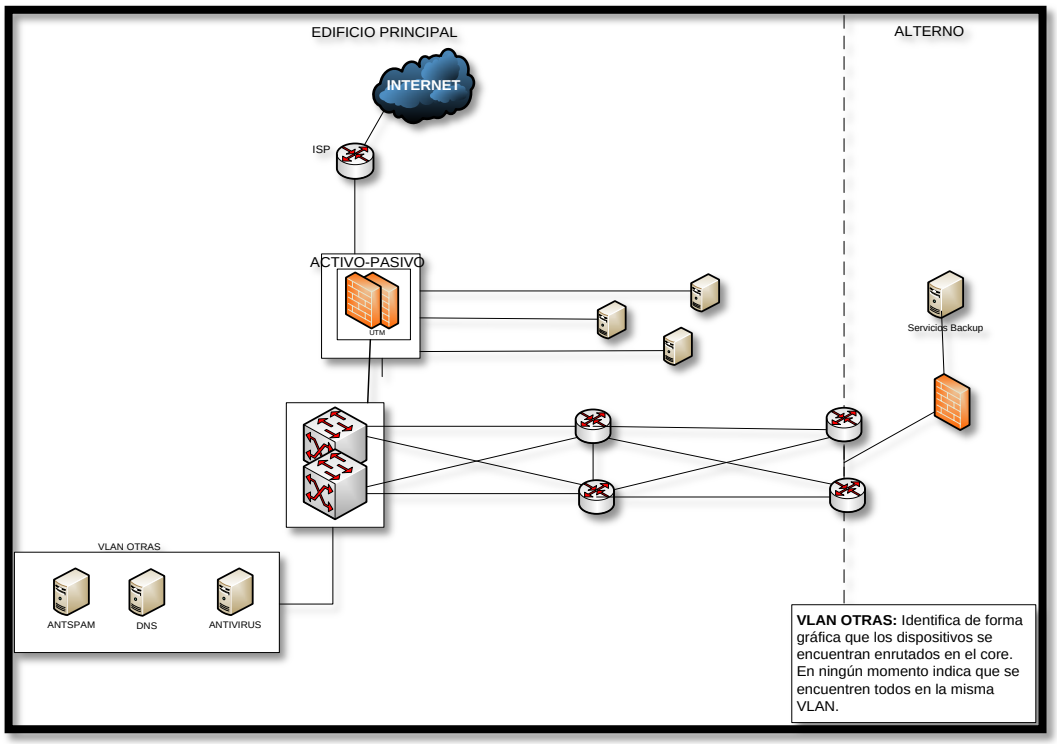
- Protecciones de Elementos de red Generales.
- Frontera Internet
- Frontera WAN
- Monitoreo, Análisis y Correlación

La evaluación se realizó sobre la arquitectura de red en funcionamiento, diagramada en la figura 6.

6.2.1 Protecciones Básicas de Red. Dentro de los ataques más frecuentes a elementos de infraestructura de red se encuentran:

- Denegación de Servicios (DoS)
- Denegación de Servicios Distribuido (DDoS)
- Accesos no autorizados
- Sesiones hijacking
- Ataque man-in-the-middle (MITM)
- Escalamiento de privilegios
- Intrusiones
- Botnets

Figura 6. Arquitectura de red evaluada



Fuente: Autores

- Ataques a protocolos de enrutamiento
- Ataques a Spanning tree
- Ataques a nivel capa 2

Para asegurar la infraestructura de red se requiere realizar un aseguramiento al acceso para la administración de estos dispositivos. Si el acceso a los dispositivos de infraestructura se ve comprometida, la seguridad y la gestión de toda la red puede verse en serios problemas. Por lo tanto, es fundamental establecerlos controles adecuados con el fin de evitar el acceso no autorizado a los dispositivos.

- Passwords Locales: Los passwords deben ser controlados por un servidor AAA. Sin embargo, en ciertos dispositivos es usual que se almacene información sensible de forma local.
- Banners de notificación: Es recomendado que un banner con una notificación legal se encuentre presente ante cualquier sesión, que asegure que los usuarios son notificados de las políticas de seguridad y a las cuales se encuentran sujetos.

- Autenticación AAA: AAA es una arquitectura para manejar un grupo de funciones de Seguridad (Authentication, Autorization and Accounting) en forma Independiente de forma modular.

- Acceso Administrativo seguro: Implementar mejores prácticas:

- Habilitar SSH en vez de Telnet.

- Evitar HTTP, si es posible usar HTTPS si es requerido.

- Deshabilitar puertos innecesarios que permitan acceso.

- Definir timeout para sesiones de administración.

Cuadro 3. Mejores prácticas e índice de riesgo para acceso lógico

Protección	**Mejor práctica**	**Estado actual**	**Índice de riesgo**
Password locales	Habilite la encripción automática de password	- Existe a nivel de los switches 3COM - Dispositivos de seguridad (AV, FW, VPN, IDS) por políticas de fábrica son encriptados. - Dispositivos de servicios corporativos (DNS, DHCP), el password maneja la encripción que ofrece el sistema Operativo	**2B**
	Defina en los dispositivos donde aplique, el password de ingreso a comandos de configuración. En lo posible esta autenticación también debe ser efectuada contra un servidor AAA.	- Dispositivos switch 3COM, por fabrica estos manejan son niveles de acceso para la configuración (un único password de acceso), la autenticación es local, no existe autenticaciones hacia un AAA habilitada - Para todos los dispositivos de seguridad exceptuando el ARCHER manejan acceso por autenticación local	**2C**
Banners	Habilitar una notificación legal se encuentre presente ante cualquier sesión	- Sobre los demás dispositivos analizados objeto de este documento no se evidencia el uso de banners	**3D**

Cuadro 3. (Continuación)

Protección	Mejor práctica	Estado actual	Índice de riesgo
Autenticación fuerte	Habilitar el uso de servidor de autenticación externo AAA	- De la información obtenida aparentemente todos los dispositivos analizados manejan autenticación en bases de datos internas. - Para el manejo de las VPNs, no se manejan todos los usuarios mediante autenticación contra el Radius.	**4C**
Acceso de administración seguro	Habilitar SSH en vez de Telnet	Todos los dispositivos analizados objeto de este documento tienen deshabilitado el uso de Telnet y solo ingresan por SSH. Sin embargo se encontró que uno de los switches de red se permite acceso por Telnet (192.xx.xx.xx)	**2B**
	Evitar HTTP, si es posible usar HTTPS si es requerido.	Todos los dispositivos de seguridad que permiten el ingreso por HTTP, están reconfigurados para acceder mediante el uso de HTTPS. Sin embargo, el firewall perimetral permite su administración por HTTPS desde Internet. Los dispositivos de networking de 3COM al parecer permiten el acceso mediante HTTP (192.xx.xx.xxx)	**4A**
	Deshabilitar puertos innecesarios que permitan acceso	Es necesario correr un escaneo para validar la apertura de puertos a nivel de los servicios con los que cuenta ANH.	**4C**
	Define timeout para sesiones de administración	Los dispositivos de seguridad mantienen el timeout de sesiones por defecto, esto es 60 min.	**2C**

Fuente: Autores

6.2.2 Infraestructura de Enrutamiento. El enrutamiento es una de las partes más importantes de una infraestructura, y por lo tanto es necesario tomar las medidas necesarias para asegurar los elementos que la ejecutan. Existen diversas formas en donde el enrutamiento puede verse comprometido ante un ataque, desde la inyección de actualizaciones ilegítimas hasta un DoS especializado.

Dentro de las mejores prácticas para generar un plan de aseguramiento a estos componentes se tiene:

- Restringir routing protocol membership: Muchos protocolos de enrutamiento, particularmente los de enrutamiento interno, implementan descubrimiento automático de sus vecinos (peer), que facilitan la configuración de los routers. Por defecto este mecanismo opera asumiendo que todos los vecinos son

confiables, haciendo posible establecer sesiones contra routers falsos y por ende inyectar datos falsos.

- Control en la propagación de rutas: La mayoría de protocolos de enrutamiento, permiten crear filtros de rutas para prevenir que rutas específicas sean propagadas a través de la red. En términos de seguridad, estos filtros son útiles porque ayudan a asegurar que solamente redes legítimas sean anunciadas.

- Registro de los cambios de estado: Frecuentes cambios de estado en la conectividad de una red son síntomas de inestabilidad. Estos síntomas también pueden indicar ataques continuos contra la infraestructura de enrutamiento. Loguear los cambios de estado en los cambios de sesiones entre vecinos es una buena práctica que ayuda a identificar problemas y facilita el troubleshooting.

Cuadro 4. Mejores prácticas e índice de riesgo para enrutamiento

Protección	**Mejor práctica**	**Estado actual**	**Índice de riesgo**
Restringir routingprotocolmembership	Habilite autenticación entre peers, mediante MD5	Normalmente ningún ISP maneja configuración de autenticación con MD5, se recomienda validar directamente con el proveedor	3B
	Realice la configuración de interfaces pasivas para permitir o prevenir la propagación de actualización de rutas por las interfaces esperadas.	Validar directamente con el proveedor la configuración de passive-interface dentro de las configuraciones de los routers.	3B
Control de propagación de rutas	Implementar filtrado por prefijo en los límites	Validar la configuración de route-map y redistribute sobre los routers	1C
Logueo de cambios de estado	Habilitar el log ante cambios de vecino	Validar con el ISP la habilitación de log-adjacency-changes y log-neighbor-changes. Validar con el ISP la habilitación de log-neighbor-changes.	2C

Fuente: Autores

6.2.3 Recuperación y Supervivencia. Existen diversos ataques par la afectación de servicio a una infraestructura de red. Dentro de las mejores prácticas a considerar se encuentra las expuestas a continuación:

- Deshabilitar servicios innecesarios: No todas las redes tienen los mismos requerimientos, por esto es fundamental conocer que es necesario y que no para mantenerlo controlado.

- Protección de Infraestructura mediante ACL (iACL): Técnica de control de acceso que protege la infraestructura de ataques internos y externos. iACL es una técnica basada en ACL extendidas.

- Port Security: Una infraestructura puede ser atacada con DoS mediante el uso de MAC flooding causando colapso de las tablas de direccionamiento MAC.

- Redundancia: Mantener redundancia en los equipos de una infraestructura elimina puntos únicos de falla, mejorando la disponibilidad de la red.

Cuadro 5. Mejores prácticas e índice de riesgo para recuperación

Protección	**Mejor práctica**	**Estado actual**	**Índice de riesgo**
Recuperación y Supervivencia	Port security	- No se evidencia manejo de aseguramiento de puertos dentro de las configuraciones de switches o routers.	**5C**
	Redundancia	- Los elementos de CORE se encuentra en HA - Los firewalls se encuentra en HA, No existe configuraciones de Alta disponibilidad hacia el centro de Computo alterno.	**4C**

Fuente: Autores

6.2.4 Telemetría de Red. Para operar y asegurar disponibilidad de la red, es importante tener visibilidad de lo que está ocurriendo sobre ésta. La telemetría es el término que se usa para referirse a las capacidades que permitiría, en unión con otras herramientas (recolección, tendencias y/o correlación), la detección de errores o posibles problemas de seguridad dentro de la red.

- Sincronización de tiempo: Esta es crítica para el análisis y correlación de eventos.

- Estadísticas de tráfico: Estas estadísticas proporcionan información base de manejo de throughput y ancho de banda, dentro de la infraestructura.

- Información de estado de los sistemas: Medición y monitoreo de las características básicas de los sistemas, como CPU y memoria.

- Syslogs: Este tipo de manejo proporciona invaluable información operacional.

- SNMP: Proporciona framework estandarizados.

Cuadro 6. Mejores prácticas e índice de riesgo para telemetría

Protección	Mejor práctica	Estado actual	Índice de riesgo
Telemetría	Sincronización de Tiempo (NTP)	- No se evidencia configuración de ningún servidor NTP al interior de ANH.	4C
	Estadísticas de tráfico	- Debido a que el monitoreo es manejado en outsourcing, no se encontraron estadísticas y uso dado al monitoreo realizado. - Cada administrador controla y monitorea las alarmas y estadísticas del módulo que gestiona.	4C
	Estado del sistema	- Cada herramienta maneja su monitoreo de sistema, y es responsable por la misma.	3C
	SNMP	- No Se evidencia el uso de SNMP	4C

Fuente: Autores

6.2.5 Aplicación de Políticas. Este punto se basa en asegurar que el tráfico que circula se encuentre acorde a las políticas de red definidas, como direccionamientos IP y tipos de tráfico. Paquetes anómalos deben ser descartados lo más cerca posible a la frontera de la infraestructura. Es acá en donde la buena creación de ACL, instalación de Firewalls e IPS perimetrales toma mayor fuerza.

- Filtrado acceso perimetral: Aplicar políticas (reglas) sobre que tráfico es permitido hacia la infraestructura de la compañía.

- Protección por IP spoofing: Involucra el descarte de paquetes que presentan un direccionamiento origen inválido.

Cuadro 7. Mejores prácticas e índice de riesgo para aplicación de políticas

Protección	Mejor práctica	Estado actual	Índice de riesgo
Filtrado acceso perimetral	ACL	Se recomienda revisión de ACL sobre los dispositivos que intervienen en la comunicación de los elementos de seguridad perimetral de la compañía.	**3C**
	Definición reglas	No se ha realizado un esquema de depuración y afinación de políticas, esto puede causar lentitud en la respuesta de los dispositivos No se evidencia un depurado de políticas, esto lleva a que las políticas son genéricas en servicios.	**5C**
Protección IP Spoofing	Spoofing interfaces de firewall	La configuración del spoofing no se encuentra generalizada (configurada) sobre todas las interfaces de los firewalls	**3B**

Fuente: Autores

6.2.6 Infraestructura de Switching. Este punto se concentra en garantizar la disponibilidad de los elementos L2 (capa2). Ver cuadro 8.

Cuadro 8. Mejores prácticas e índice de riesgo para switching

Protección	Mejor práctica	Estado actual	Índice de riesgo
Restringir dominios de broadcast	VLAN	En general las configuraciones de los dispositivos y diseño de la arquitectura, muestra la segmentación de la red mediante el uso de VLANs	1B
Seguridad STP	Deshabilitar VLAN dynamic trunk negotiation	Sobre los switches 3COM, se evidenció la configuración de edge-port (portfast en ambiente cisco) lo que da mayor velocidad de intercambio a la interfaz	1B
	Deshabilitar los puertos que no se usan y configurarlos en una VLAN de no producción	Se observaron puertos a nivel de switch deshabilitados pero no se tiene el uso de una VLAN de no producción estándar para agruparlas, sin embargo, dentro de las políticas de cambio internas de la compañía, cuando ciertas interfaces se liberan (se encontraban en uso) estas son movidas a una VLAN de no producción pero no son apagadas.	5C

Fuente: Autores

- Restringir dominio de broadcast: Dentro de las mejores prácticas se encuentra el segmentar la red en diversos dominios de broadcasts (VLAN o IP subnets). Al realizar esta segmentación se recomendó seguir el principio de diseño jerárquico, el cual ayuda a generar una red escalable.

- Seguridad Spanning Tree Protocol: STP (IEEE 802.1D) es un protocolo de administración de enlaces a nivel 2. STP proporciona redundancia de caminos mientras previene loops indeseados. Lamentablemente STP no implementa ni autenticación ni cifrado para el intercambio de BPDUs, debido a esto cualquiera que hable STP puede llegar a interactuar con los switches que lo tengan configurados, permitiendo que un atacante inyecte falsos BDPU, generando un recalculo en la topología o simplemente leer los BPDU que circulan y obtener datos relevantes de la topología.

6.2.7 Mitigación de Amenazas a la Infraestructura. Las amenazas que se pueden llegar a mitigar configurando de forma correcta los dispositivos, se describen en el siguiente cuadro.

Cuadro 9. Mitigación de amenazas a la infraestructura

	Dos	**Ddos**	**Acceso no autorizado**	**Intrusiones**	**Ataques al protocolo de enrutamiento**	**Ataques l2**	**Visibilidad**	**Control**
AAA			Si	Si			Si	Si
Autenticación SNMP			Si	Si			Si	Si
SSH			Si	Si			Si	Si
Fuertes políticas de manejo de password			Si	Si				Si
ACL por sesiones	Si	Si	Si	Si			Si	Si
Autenticación de Routers vecinos	Si		Si		Si			Si
RouteFilterin g	Si		Si		Si			Si
Redundancia Topológica	Si	Si			Si	Si		Si

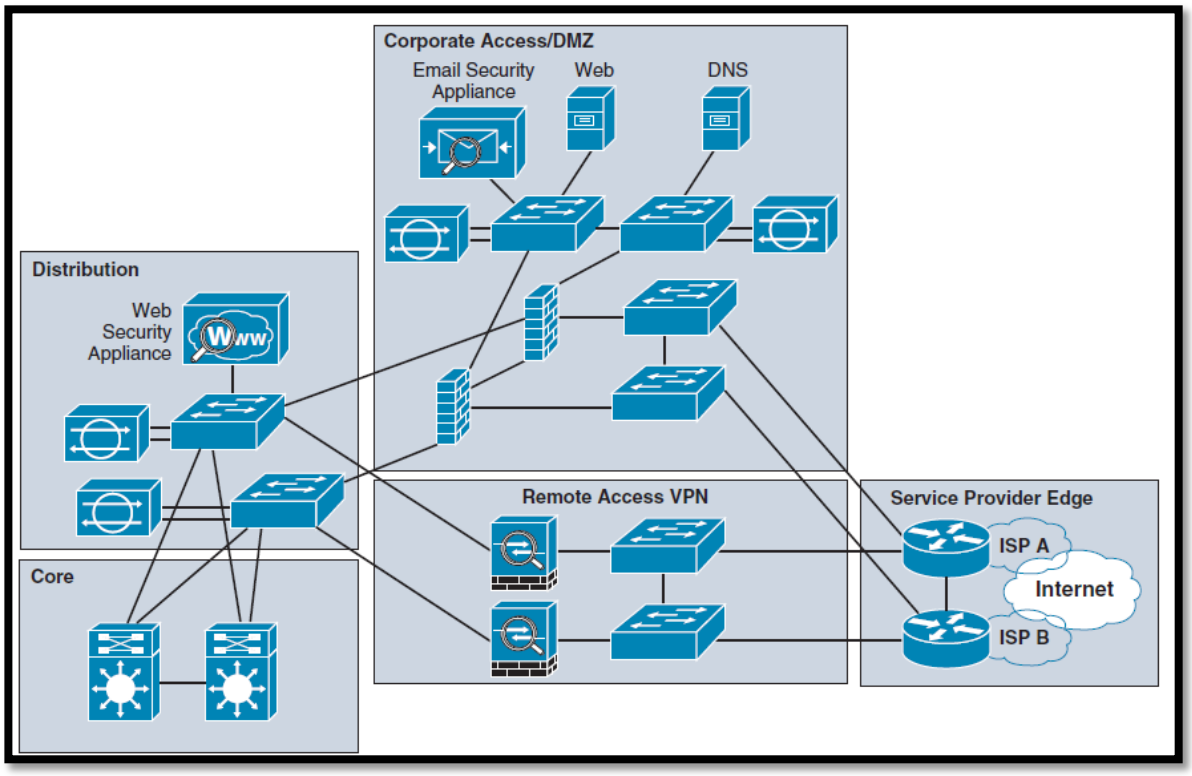
Fuente: Autores

6.2.8 Frontera de Internet. Dentro del análisis de seguridad perimetral, es fundamental realizar el análisis puntual de la infraestructura que funciona como gateway entre la compañía y el Internet. Un diseño apropiado de esta frontera es

fundamental para asegurar la disponibilidad de los servicios de Internet a toda la compañía.

La siguiente figura presenta un esquema generalizado de cómo deberían interconectarse los dispositivos de infraestructura de borde hacia Internet.

Figura 7. Esquema generalizado de protección perimetral en Internet



Fuente: Cisco SAFE Reference Guide. Cisco ValidatedDesign. July 8, 2010

La frontera de Internet puede ser dividida en varios bloques funcionales. Cada bloque funcional maneja sus propios criterios de diseño y seguridad.

- Límite contra ISP: Este límite se compone de enrutadores de frontera, los cuales no solo enrutan el tráfico entre la red interna y externa, sino que se considera como la primera línea de defensa contra ataques externos. Dentro de las consideraciones de diseño, es recomendable manejar redundancia en canal de Internet.

- Acceso corporativo y DMZ: Los firewalls proporcionan control de acceso statefull y Deep packetin spection. Los firewalls perimetrales fueron diseñados para proteger los datos y recursos de la organización de ataques externos mediante el acceso controlado a servicios públicos ubicados en redes DMZ. Esta protección se realiza manejando la aplicación de políticas de acceso,

manteniendo trazabilidad del estado de las conexiones e inspección del paquete. Dentro de los servicios perimetrales que se encuentran en una DMZ son los appliance o aplicaciones de seguridad para el manejo de e-mail, DNS y FTP. Asi como los Web Application Firewall (WAF) para protecciones específicas de aplicaciones claves del negocio.

- Acceso Remoto VPN: Una de las capas esenciales en el manejo de frontera es el proporcionar acceso seguro a los accesos remotos. Para este punto existen varias consideraciones, dependiendo de las políticas de seguridad internas de la compañía, depende de estas escoger los criterios para trabajar VPN SSL o VPN IPSec.

- Distribución: La capa de distribución contempla los switches que dan la conexión entre el firewall perimetral con el core de la compañía. De igual forma dentro de esta capa de distribución se encuentran los servicios de seguridad como el URL Filtering, contentinspection e IPS proxys.

Cuadro 10. Mejores prácticas e índice de riesgo para frontera Internet

Dispositivo	Mejor práctica	Estado actual	Índice de riesgo
IPS	Se recomienda que se encuentre lógicamente ubicado entre el firewall de frontera y el Core	En la actualidad ANH posee la funcionalidad de IPS perimetral dentro del sistema UTM perimetral. No mantiene una interfaz exclusiva de administración.	**5B**
	Administración de alertas y monitoreo		
	Dispositivo en redundancia		
	Use una interfaz exclusiva para administración		
Firewall	Se recomienda que la política habilitada para salida a Internet (servicios Internet HTTP, HTTPS, FTP, entre otros) sea para dirección IP fuente Proxy.	Las reglas de navegación se encuentran genéricas (Any-Any) tanto para los equipos proxy como para equipos internos. Aunque se encontraron controladas por grupos LDAP de navegación	**1C**
	Dispositivo en redundancia	El firewall perimetral se encuentra en redundancia. Sin embargo no maneja esquema de Alta disponibilidad activo-activo, ni con el Centro de Datos alterno.	**4B**

Cuadro 11. (Continuación)

Dispositivo	Mejor práctica	Estado actual	Índice de riesgo
Firewall	No permitir administración por Telnet y HTTP solo SSH y HTTPS	Solo maneja SSH Y HTTPS, sin embargo se encuentran habilitados sin control sobre el acceso a internet. O hay restricción desde donde pueden ser administrados.	**4B**
	Habilitar funciones de telemetría (NTP, log,	No existe sincronización a algún servidor NTP	**5B**
	Use una interfaz exclusiva para administración, protegida de accesos.	No se maneja interfaz exclusiva de administración.	**5B**
	Regla que permita el tráfico entre el Antispam y el DNS externo	No se evidenció la regla.	**1D**
	Reglas que peritan la actualización del Antispam	No se evidenció la regla	**1D**
URL Filtering	Todo trafico WEB debe ser verificado por el URL Filtering	Se maneja cobre el dispositivo UTM perimetral.	**3C**
	Mantenga un manejo lo más granular posible (por usuarios, categorías, entre otras)	La granularidad sobre un dispositivo UTM no es amplia.	**3C**
	Configure y revise los reportes generados, reenvíelos a un correlacionador	No se encontró evidencia del análisis de log de la herramienta. Sin embargo el control de navegación es hecho mediante grupos de LDAP.	**3C**
	Use una interfaz exclusiva para administración	No se maneja un interfaz exclusivo para administración.	**5B**
UTM	Dispositivo en redundancia	El UTM perimetral se encuentran en redundancia. Sin embargo no maneja esquema de Alta disponibilidad activo-activo, ni con el Centro de Datos alterno.	**4B**
WAF	Configurar WAF para aplicaciones críticas (como aplicaciones transaccionales)	No se tiene evidencia que exista WAF.	**5B**
Proxy	Todos los browser de la compañía deben estar apuntando al proxy.	ANH no posee proxy para navegación	**3D**
E-mail Security (Antispam)	Dispositivo en redundancia	Se encuentra en redundancia	**1C**
	Una dirección estática debe ser definida en el Firewall, la cual debe manejar NAT entre la dirección pública y la dirección privada	El servidor (antispam) tiene configurada una dirección pública en el Firewall. No se evidencia el uso de NAT.	**3C**

Cuadro 12. (Continuación)

Dispositivo	Mejor práctica	Estado actual	Índice de riesgo
	Antispam debe tener configurado acceso al DNS externo.	Tiene permisos ANY para protocolo 53	**1D**
	Debe estar configurado para estar actualizado en forma constante	Se encuentra configurado para realizar actualizaciones todos los días desde 00:00 horas cada 10 minutos	**1B**
	Servidor SMTP debe apuntar al Antispam para asegurar el control de los correos	Se encuentra configurado.	**1B**
	Use una interfaz exclusiva para administración	No se utiliza una interfaz independiente para administración.	**5B**
VPN	Dispositivo en redundancia	Se encuentra en redundancia.	**5B**
	Use un sistema AAA para la autenticación de los usuarios remotos	Se tiene autenticación con usuario LDAP para las VPNs SSL	**1B**
	Use una interfaz exclusiva para administración	No se maneja una interfaz independiente para administración	**5B**

Fuente: Autores

6.2.9 Mitigación de Amenazas al Perímetro de Internet. Las amenazas que se pueden llegar a mitigar usando de forma correcta los dispositivos de protección perimetral en Internet se describen en el Cuadro 11.

6.2.10 Frontera WAN. Como WAN se pueden agrupar a todas las conexiones que la ANH recibe de terceros, es por esto que la disponibilidad y seguridad sobre estos enlaces y tráfico, es crucial para la operación del negocio.

El objetivo, desde una perspectiva de seguridad, es lograr que la compañía reciba con plena confianza los servicios globales que necesita para llevar los objetivos del negocio. Éste se logra a través del enfoque en defensa en profundidad discutido anteriormente.

Dentro de las amenazas más comunes que se encuentran direccionados a una arquitectura WAN se pueden llegar a identificar tres áreas claves. En el siguiente cuadro se especifican en conjunto con el objetivo de seguridad y los elementos necesarios para lograr mitigarlos.

Cuadro 13. Mitigación de amenazas al perímetro de Internet

	Ddos/dos/ worms	Accesos no autorizados	Spyware/malware/phishing/spam	Network abuse/intrusion	Amenazas capa de aplicación	Visibilidad	Control
IPS	Si		Si	Si	Si	Si	Si
Firewall	Si	Si		Si		Si	Si
Antispam (e-mail security)			Si			Si	Si
URL Filtering (web Security)	Si	Si		Si		Si	Si
Aplication Control					Si	Si	Si
Web Application Firewall					Si	Si	Si
Enrutamiento Seguro	Si	Si		Si		Si	Si
Switching seguro	SI	SI		SI		SI	SI

Fuente: Autores

Cuadro 14. Amenazas claves en WAN

Amenaza	Amenazas mitigadas	Objetivos de Seguridad	Elementos de Seguridad
Actividad maliciosa de clientes	Proliferación de Malware, botnets, worms, virus, troyanos. Abuso de la red y aplicaciones	Detectar y mitigar las amenazas.	- Integración con un IPS - Telemetría
Amenazas enlaces de tránsito	Acceso no autorizado a la red y a los datos a través de ataques de sniffing o Man-in-the-middle (MITM)	Aislar y asegurar los datos y accesos WAN	- Conectividad WAN segura
Amenazas contra la infraestructura	Accesos no autorizados a los dispositivos, red y datos. DoS	Ofrecer servicios flexibles y de alta disponibilidad	- Enrutamiento seguro - Control de políticas de red - Switching seguro - Acceso seguro - Telemetría

Fuente: Autores

A continuación se describen las mejores prácticas para lograr cubrir los objetivos de seguridad anteriormente definidos.

Conectividad WAN Segura: El objetivo es proporcionar confidencialidad, integridad y disponibilidad de los datos que transitan a través de la WAN. El diseño e implementación de una conectividad de WAN segura está direccionada al sistema

end-to-end. Las recomendaciones de diseño[23] claves para asegurar la conectividad segura se basa en:

- Aislar tráfico WAN
- Autenticar acceso WAN
- Encriptar el Acceso WAN

Cuadro 15. Mejores prácticas e índice de riesgo para frontera WAN

Dispositivo	Mejor práctica	Estado actual	Índice de riesgo
IPS	Se recomienda instalar el IPS después del terminador de VPNs, para asegurar que el IPS reciba el texto claro y tráfico no modificado para el monitoreo.	En la actualidad ANH no posee un IPS para WAN. Todo se encuentra conectado al UTM perimetral	**5B**
	Administración de alertas y monitoreo		
	Alta redundancia		
Telemetría	Idem 6.2.4 Telemetría de Red	- Idem - 6.2.4 Telemetría de Red	**Idem**
Conectividad WAN Segura	VPN para aislar el tráfico o enlaces dedicados	Las VPN se manejan sobre los firewalls. No todo el tráfico va encriptado, algunos enlaces llegan de forma independiente.	**4C**
	PKI para autenticación fuerte		
	AES para inscripción fuerte		

Fuente: Autores

6.2.11 Mitigación de Amenazas a la WAN. Las amenazas que se pueden bloquear usando de forma correcta los dispositivos de protección perimetral en la WAN se describen en el cuadro 14.

6.2.12 Monitoreo, Análisis y Correlación. Como ya se comentó a lo largo de este documento, el enfoque en defensa en profundidad se basa en la implementación de múltiples medidas de seguridad en capas a lo largo de la red y la influencia de la infraestructura de red (routers, switches) como herramientas de seguridad para ayudar a reforzar dichas capas.

[23] Es claro que la escogencia del tipo de tráfico al que se le aplican las recomendaciones de diseño son derivadas del estudio previo del tipo de tráfico que se manejan a través de los diversos enlaces y su criticidad.

Cuadro 16. Mitigación de amenazas al perímetro de WAN

	Botnets	DoS	Accesos no autorizados	Malware/Spyware	Application, Network Abuse	Fuga de Datos	Visibilidad	Control
Conectividad WAN Segura			Si			Si		Si
Routing seguro		Si	Si				Si	Si
Redundancia		Si	Si					Si
Firewall	Si		Si		Si	Si		Si
IPS	Si			Si	Si			Si
Switching seguro		Si	Si		Si	Si		
Acceso Seguro			Si			Si	Si	Si
Telemetría	Si	Si	Si	Si	Si		Si	

Fuente: Autores

Dentro de cada una de las áreas verificadas (Protecciones de red básicas, Internet y WAN), se analizó la importancia de tener telemetría, como una herramienta útil para obtener una visibilidad consistente y exacta de los que sucede en la red. Sin embargo estos logs y eventos, no pueden quedar aislados; para garantizar un ambiente seguro es aconsejable manejar una herramienta que permita agruparlos, analizarlos y correlacionarlos al unísono, para identificar no solo posibles problemas de red, sino identificar o prever incidentes de seguridad y amenazas.

Un elemento de monitoreo, análisis y correlación de eventos debe llevar a que un administrador de red y/o seguridad sea capaz de:

- Identificar Amenazas
- Confirmar elementos comprometidos por un ataque
- Reducir falsos positivos
- Reducir la cantidad de información de eventos
- Determinar la severidad de un incidente
- Reducir el tiempo de respuesta

6.3 RECOMENDACIONES

Basado en las no conformidades relevadas en el diagnóstico de Seguridad en la actual Arquitectura, el Levantamiento de Información y teniendo en cuenta los

controles asociados al cumplimiento de la ISO 27002, se presentan las siguientes recomendaciones:

Cuadro 17. Mejores prácticas e índice de riesgo para Monitoreo

Dispositivo	Mejor práctica	Estado actual	Índice de riego
Monitoreo, Análisis y correlación	Se recomienda tener un dispositivo centralizado para administrar los eventos y tráfico de los dispositivos	La ANH cuenta con un dispositivo que cumple esta función, sin embargo este dispositivo está en un nivel de madurez en configuración básico.	5C

Fuente: Autores

6.3.1 Recomendaciones asociadas a cumplimiento ISO/IEC 27002

Cuadro 18. Recomendaciones de acuerdo a ISO 27002

Ítem	Control	Recomendación
ISO/IEC 27002 – Ítem 7.1.1	Se debe mantener un Inventario de los activos de Información	Este control se debe implementar de la siguiente forma: 1.Identificación de los activos, identificando el tipo de activo (información, software, físico, servicio, gente) 2. Listado de los activos con su tipo, formato, localización, información de backup, información de licencia y valor para el negocio. 3. Asignar un responsable y documentarlo dentro del inventario. 4. Desarrollo de reglas para el mantenimiento y actualización del inventario.
ISO/IEC 27002 – Ítem 10.10.1	Logs de Auditoria deben ser estandarizados	Este procedimiento se puede estandarizar con el siguiente procedimiento: 1.Estandarice los registros de log de auditoría de usuarios y de eventos generados por los sistemas de seguridad de la información, con información relevante como: User ID, fechas, horas, detalles claves del evento, terminal que lo genera, cantidad de accesos satisfactorios o rechazados al sistema, cambios a la configuración del sistema, uso del sistema, archivos accedidos y tipos de acceso, direcciones de red y protocolos, alarmas activadas por control de acceso al sistema, habilitación o des-habilitación de protecciones al sistema (como Av, IPS..)

Cuadro 16. (Continuación)

Ítem	Control	Recomendación
	Ciertos registros de auditoría y eventos de seguridad relevantes deben ser mantenidos por un periodo de tiempo definido.	Este control puede ser implementado con el siguiente procedimiento: 1. Defina un periodo de retención para cada grupo de logs de auditoría. Típicamente esta definición es basada en: Determinación establecida por el personal de regulación de la compañía, requerimientos contractuales y análisis de riesgos. 2. Mantenga los logs de auditoría almacenados en lugares apropiados. 3. Verifique la integridad de los logs al menos una vez al año.
ISO/IEC 27002 – Ítem 10.10.2	Logs de auditoría deben ser revisados periódicamente	Este control puede ser implementado con el siguiente procedimiento: 1. Establecer los procedimientos para la revisión de los logs de auditoria, considerando los siguientes factores de riesgo: Criticidad de los procesos, valor, sensibilidad y criticidad de la información involucrada y experiencia pasada de accesos no autorizados y la frecuencia con la cual las vulnerabilidades son explotadas.
ISO/IEC 27002 – Ítem 10.10.3	Logs de auditoría deben ser protegidos apropiadamente	Este control puede ser implementado con el siguiente procedimiento: 1. Implementar una infraestructura segura para almacenar los logs. 2. Documentar los procedimientos
ISO/IEC 27002 – Ítem 10.10.6	Los reloj de todos los sistemas deben estar sincronizados	Este control puede ser implementado a través del siguiente procedimiento: 1. Implementar un mecanismo, el cual permita sincronizar los relojes con un tiempo estándar confiable. 2. Defina rutinas de verificación de inconsistencias y correcciones de variaciones de tiempo significativas.
ISO/IEC 27002 – Ítem 10.3.2	Criterios de aceptación deben ser establecidos para nuevos sistemas, actualizaciones y nuevas versiones.	Este control puede ser implementado a través del siguiente procedimiento: 1. Establecer un proceso de acreditación y certificación formal para verificar que los requerimientos de seguridad, han sido apropiadamente direccionados, incluyendo: requerimientos de capacidad y desempeño Planes de contingencia, procedimientos de reinicio y recuperación ante errores Procedimientos de preparación pruebas de rutina Manual de procedimientos Requerimientos de continuidad del negocio 2. Obtener aprobación formal para implementar los cambios.

Cuadro 16. (Continuación)

Ítem	Control	Recomendación
ISO/IEC 27002 – Ítem 11.2.3	Un procedimiento de administración de passwords debe ser implementada	Este control puede ser implementado a través del siguiente procedimiento: 1.Manejo de password correctamente: Requerir y asegurar cambio de password periódicamente Restringir reúso de password 2.Adminstración de password temporales
ISO/IEC 27002 – Ítem 11.4.2	Accesos remotos a la red deben ser autenticados	Este control puede ser implementado adoptando métodos de autenticación compatibles con el nivel de seguridad asignado a la información.
ISO/IEC 27002 – Ítem 11.4.4	Diagnóstico y configuración de puertos debe ser protegida contra accesos no autorizados	Este control puede ser implementado a través del siguiente procedimiento: 1. Implementar un procedimiento de bloqueo de puertos. 2. Deshabilitar o quitar puertos, servicios o similares que no sean requeridos por la funcionalidad del negocio.
ISO/IEC 27002 – Ítem 11.4.4	Se deben establecer mecanismos para reportes y registros (logs) de eventos de seguridad de la información	Este control puede ser implementado a través del siguiente procedimiento: 1.Establezca procedimientos para manejo de eventos de seguridad, incluyendo: Definición de eventos y sus respectivas clases, Definición de responsabilidades para tratar eventos, Planes de respuesta a varios tipos de eventos, Análisis e identificación de las causas de los incidentes, Planeación e implementación de medidas para prevenir recurrencias, Colección, retención y protección de registros de auditoría y evidencias similares.

Fuente: Autores

6.3.2 Recomendaciones técnicas asociadas al cumplimiento mejores prácticas evaluadas.

Cuadro 19. Recomendaciones de acuerdo mejores prácticas

Id – mejor práctica	Recomendación	Justificación
6, 7,33-Administración segura	Validar sobre todos los dispositivos de networking deshabilitar el posible acceso por Telnet y HTTP.	-Asegurar la protección de las credenciales de los administradores. -Previene ataques de suplantación.

Cuadro 17. (Continuación)

Id – mejor práctica	Recomendación	Justificación
32,42,51 – Redundancia (Disponibilidad)	Generar un plan para activación de Alta disponibilidad entre los tres dispositivos de seguridad perimetral existentes.	-Apoya el plan de continuidad del negocio -Mejora la disponibilidad de los servicios y la hace resistentes a ataques -Mejora la escalabilidad de la infraestructura mediante el uso de balanceo de servicio. - Mantiene una alta disponibilidad automática, minimizando los tiempos de restablecimiento del servicio.
26,54 – IPS	Realizar un estudio para validar la eficacia del IPS dentro del UTM perimetral.	-Prevención reactiva de ataques maliciosos. - Trazabilidad de exposición de la organización a ataques. - No se castiga el desempeño de las otras funcionalidades como los son el firewall.
34- Habilitar funciones de telemetría en los Firewalls	Configurar el servicio de NTP de los dispositivos, y que este sea sincronizado a un NTP externo.	-Validez de los datos ante cualquier evento de auditoría. -Trazabilidad de eventos de seguridad por flujo de información.
35,41,50,53- Interfaz de administración independiente	Crear una red administración protegida por firewall y no enrutada en el CORE.	-Mayor control de acceso interno a la BD de las políticas de seguridad que se encuentran ejecutando en todos los firewalls. -Menor probabilidad que la management sea atacada por malware que se puedan filtrar por redes enrutadas dentro del CORE. -Aplicación de Defensa en profundidad, pues no solo deja el nivel de control de acceso a la management sino que es controlada por políticas de seguridad.
43 - Tener WAF para aplicaciones web críticas.	Los servicios WEB, deben ser protegidos.	-Prevención reactiva ante ataques específicos dirigidos a este tipo de servicios. -Permite generar un control del tráfico realmente válido, mediante el uso de “whitelist”
8,14,21,25 – Recuperación y supervivencia	Es necesario iniciar un proceso de hardening en primera instancia sobre todos los servidores de ANH como los son DNS, DHCP, Mail.	-Elimina el único punto de falla que tiene los administradores para ingreso ante una emergencia.

Cuadro 17. (Continuación)

Id – mejor práctica	Recomendación	Justificación
21 – Definición reglas	Realizar una depuración y definición más cerrada de las reglas. Dentro de la depuración se recomienda analizar cuáles son las reglas más usadas y su orden.	-Evita accesos no autorizados a la red -Mejora el desempeño de los firewall -Mejora la administración y auditoria del tráfico analizado.
25 - Port security	Habilitar por security sobre los puertos o generar	-Previene ataques DoS basados en MAC flooding[24] -Previene ataques de overflow sobre las tablas de MAC address.
61 - Se recomienda tener un dispositivo centralizado para administrar los eventos y tráfico de los dispositivos	Configurar el dispositivo centralizado para administrar los eventos y tráfico de los dispositivos	-Permite reaccionar reactivamente ante posibles ataques y tomar medidas preventivas. -Permite mantener una trazabilidad de los eventos de seguridad centralizados para ser analizados al unísono -Mantiene centralizado los eventos de seguridad en caso de requerir una auditoria.
19 – SNMP	Se recomienda habilitar SNMPv3	-Asegura confidencialidad de la información -Asegura la integridad de los datos transmitidos por SNMP.
5- Autenticación fuerte	Habilitar un servidor AAA e iniciar un plan de autenticación fuerte para los servicios prioritarios	-Garantiza autenticación y manejo de perfiles de forma centralizada. -Permite tener centralizados los eventos.

Fuente: Autores

Como recomendación general se elaboró el diagrama de arquitectura de seguridad de la red apropiada para la entidad. Ver figura 8.

6.4 ANÁLISIS DE VULNERABILIDADES TÉCNICAS

Al inicio de la operación se llevó a cabo una evaluación del estado actual de la configuración y arquitectura del Servidor para VMM (Vulnerability Manager McAfee v7.5) en la ANH, con el fin de presentar a la gerencia de TI las recomendaciones o mejoras a implementar durante el desarrollo del proyecto.

[24]MAC flooding provocaría un overflow de las tablas de MAC Address

6.4.1 Hoja de Vida

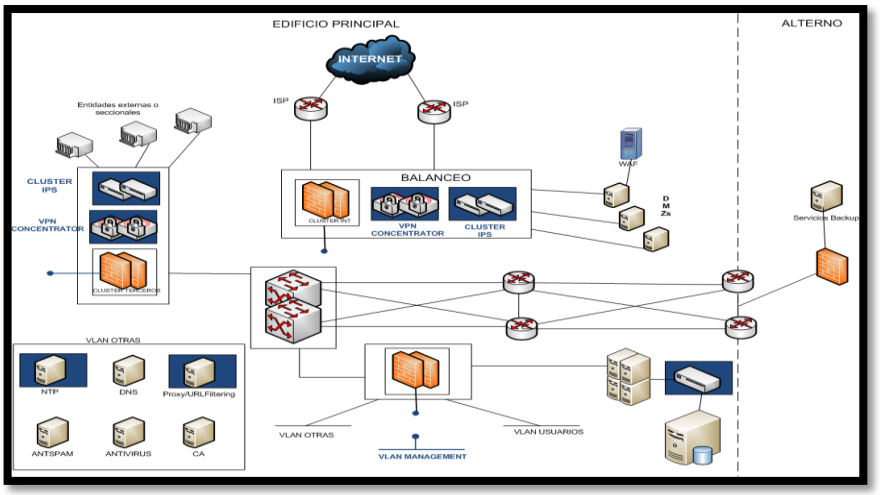
Servidor	Appliance MVM3100
Procesador	Xeon X3450 2.66 Ghz
Memoria	8Gb
Disco duro	Disco C: Boot (100 GB) Disco D: Data (365 GB)

Sistema Operativo	Windows Server 2008 R2 Standard SP1
Plataforma	64 bits
Base de Datos	SQL Server 2005 SP2
Herramienta de Vulnerabilidades	McAfee Vulnerability Manager v 7.5

Configuración de Red

Dirección IP	192.xxx.xx.xx
Máscara de Red	255.255.xx.xx
Puerta de Enlace	192.xxx.xx.xx
DNS Primario	192.xxx.xx.xx
DNS Secundario	192.xxx.xx.xx

Figura 8. Arquitectura de seguridad de red propuesta para la ANH



Fuente: Autores

6.4.2 Licenciamiento. El licenciamiento de la herramienta se encuentra activo para 1300 IPs de las cuales se están usando 122. No se tiene activo el módulo de escaneo de Aplicaciones Web. La fecha de vencimiento de la licencia que se muestra en la configuración es 26 de Febrero de 2053.

6.4.3 Actualizaciones. El Appliance cuenta con los parches de sistema operativo y las reglas de vulnerabilidades actualizadas a 22 de mayo de 2013 gracias a la visita trimestral de mantenimiento que realizó el proveedor (con contrato vigente de soporte y mantenimiento de la herramienta) en esa fecha.

6.4.4 Backups. El backup de la Base de datos de la herramienta se realiza a nivel del sistema operativo, y el último fue realizado en la visita de mantenimiento del 22 de mayo.

6.4.5 Funcionalidades por Activar. De acuerdo con la revisión realizada, todas las funcionalidades con las que cuenta la herramienta a nivel de licenciamiento se encuentran activas actualmente con excepción de la Web ApplicationsScan: McAfee Vulnerability Manager provee una configuración de escaneo, chequeo de vulnerabilidades y reporte de escaneos para Aplicaciones Web. El escáner de aplicaciones web busca vulnerabilidades que incluyen buffer overflows, crosssite scripting y acceso no autorizado. Cuando el escáner de aplicaciones web crea un activo lo asocia a una URL y no a la dirección IP del Servidor Web.

6.4.6 Alertas Actuales. De acuerdo con el historial de la herramienta, se realizaron los siguientes escaneos:

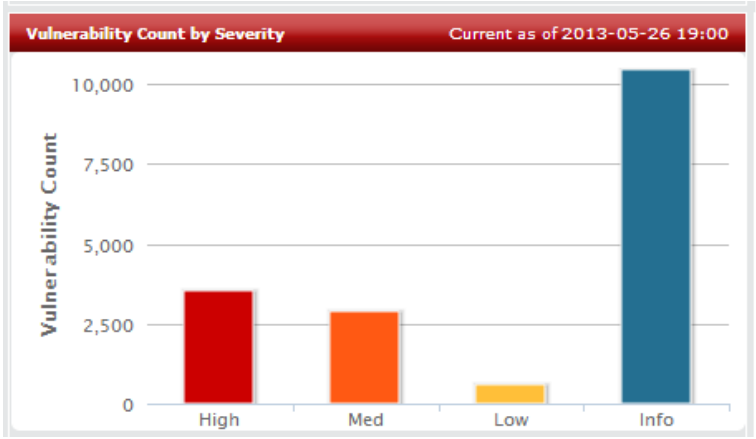
- Windows Server Scan: Realizado el 9 de mayo de 2013
- Linux Server Scan: Realizado el 9 de mayo de 2013
- QuickScan_jensyleo: Realizado el 26 de abril de 2013
- SwitchScan: Realizado el 22 de marzo de 2013

Estos escaneos arrojaron los siguientes resultados:

Tipo de Vulnerabilidad	Total
Altas	3562
Medias	2926
Bajas	647
Información	10507

Conteo de vulnerabilidades por Severidad.

Figura 9. Reporte inicial de vulnerabilidades técnicas



Fuente: Reporte de vulnerability Manager McAfee v7.5

Vulnerabilidades Altas más prevalentes:

Figura 10. Reporte inicial de vulnerabilidades técnicas

Fuente: Reporte de vulnerability Manager McAfee v7.5

Todas estas vulnerabilidades fueron asignadas vía tickets a los administradores de plataformas.

6.4.7 Recomendaciones. Se realizaron las siguientes recomendaciones:

- Grupos de Activos: En la actualidad los grupos de activos están orientados hacia los sistemas operativos que tienen instalados: Servidores Windows, Servidores Linux, Switches. Basados en las mejores prácticas para la

herramienta, se recomienda crear los grupos de activos considerando el valor que tiene para el negocio este activo en particular, es decir los grupos deben crearse de acuerdo a la criticidad del activo. Para esto se requiere realizar una clasificación de activos de información para poder determinar que grupos se asignarán y reasignar activos.

- Planeación de remediación: Concertar con los administradores de las plataformas los tiempos de remediación de las vulnerabilidades críticas, medias y bajas, que actualmente se encuentra configurado en 15, 30 y 60 días respectivamente. Después de realizar un primer escaneo con unas nuevas métricas, se podrá tener un valor real de la cantidad de vulnerabilidades a atacar y así estimar un tiempo real para solucionar las mismas.

- Remediación: Realizar la remediación de las vulnerabilidades iniciando primero por las Altas, y después pasar a las medias y bajas. En la actualidad se están generando tickets para vulnerabilidades medias y altas, y la cantidad es considerablemente elevado (más de 4000) para poder cumplir los tiempos de remediación previstos en la configuración actual.

- Escaneos periódicos: Realizar escaneos iniciando por aquellos equipos que se consideren críticos para la organización. Algunos de los escaneos a realizar son:

- SANS/FBI Top 20 Scan: Este scan busca solo las vulnerabilidades que han sido identificadas por el FBI como el top 20 de vulnerabilidades más comunes.

- Single VulnerabilityScan: Se usa para chequear una vulnerabilidad en particular.

- Full Vulnerability Scan: Scan completo de vulnerabilidades.

- WWW Application Assessment Scan: Busca en la red aplicaciones web. Prueba la aplicación web, busca debilidades y debilidades que podrían permitir acceso a la red, y busca varias vulnerabilidades asociadas con aplicaciones web.

- Automatización: Programar la ejecución automática, programada y periódica de escaneos de acuerdo con el levantamiento de información realizado para grupos de activos y cantidad de vulnerabilidades altas encontradas. Tentativamente se propone una periodicidad inicial de 6 meses.

- Notificación: Activar las notificaciones vía email con el fin que los administradores de plataforma tengan una visualización de las vulnerabilidades a remediar sobre los servidores/equipos que gestionan.

- Backups: Revisar la ejecución de los Backups, ya que estos no funcionan automáticamente y se encuentran en el mismo disco duro del servidor.

- Aplicaciones WEB: A largo plazo adquirir y activar la funcionalidad de Web ApplicationScan.

6.5 CONCLUSION

La ANH cuenta con una herramienta para Análisis de Vulnerabilidades de última generación instalada, en ejecución y actualizada, sin embargo no se está sacando provecho de la misma. Se propone la reconfiguración y un nuevo enfoque de la herramienta, de tal forma que sirva como métrica y apoyo para medir la seguridad de la red y no simplemente un reporte periódico de vulnerabilidades pendientes por remediar.

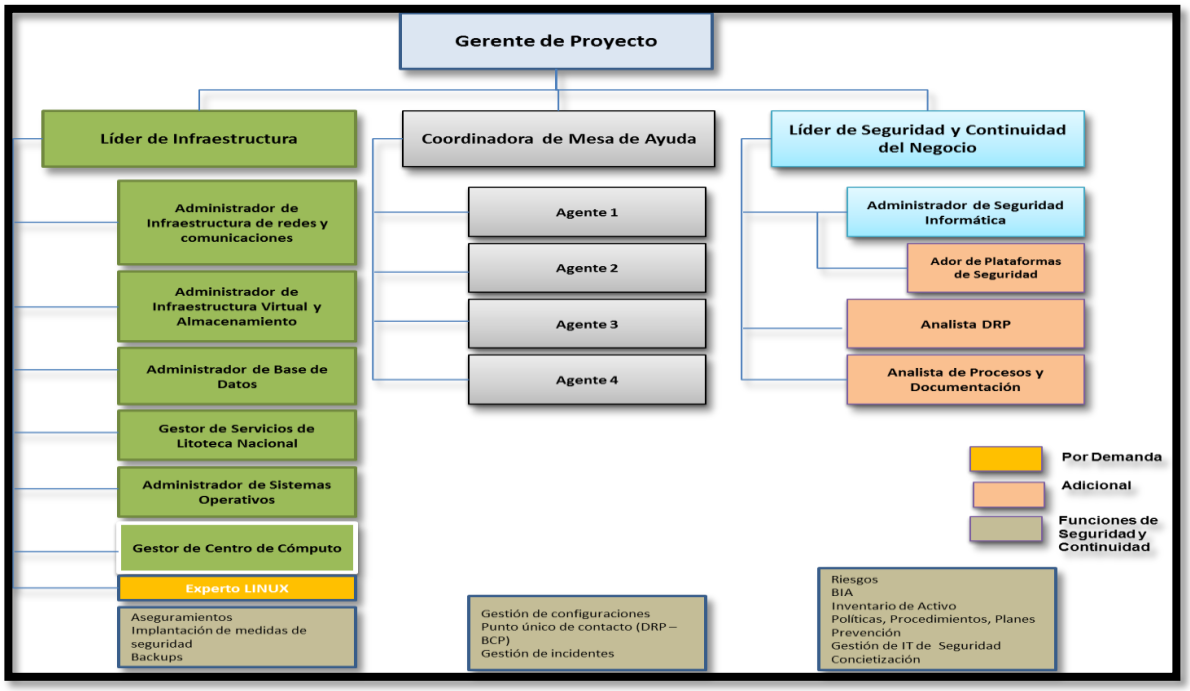
6.6 PLAN DE ACCION IMPLEMENTADO

6.6.1 Organización y plan de trabajo. Frente a las vulnerabilidades y amenazas encontradas en las evaluaciones se emprendieron las siguientes acciones, con base en las recomendaciones del SANS INSTITUTE para ciberseguridad, quien en conjunto con la Agencia Nacional de Seguridad (NSA) definieron los 20 controles críticos, los cuales se pueden consultar con mayor nivel de detalle en http://www.sans.org/critical-security-controls. Estos controles se trabajaron gracias a la conformación de un equipo de trabajo interdisciplinario. Ver figura 11.

- Inventario de dispositivos autorizados y no autorizados: Gestionar todos los dispositivos de hardware en la red para que sólo los dispositivos autorizados tengan acceso y dispositivos no autorizados y no administrados se controlen apropiadamente.

- Inventario de Software Autorizado y no autorizado: Gestionar activamente todo el software en la red de forma que sólo el software autorizado este instalado y se puede ejecutar y que el software no autorizado y no administrado se erradique de la infraestructura.

Figura 10. Equipo de trabajo para la gestión y operación de TI, Seguridad y DRP



Fuente: Autores

- Configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores: Establecer, implementar y gestionar activamente la configuración de seguridad de las computadoras portátiles, servidores y estaciones de trabajo mediante una rigurosa gestión de la configuración y cambiar el proceso de control con el fin de evitar que los atacantes exploten los servicios vulnerables.

- Evaluación continúa de vulnerabilidades y Remediación: Continuamente adquirir, evaluar y tomar una decisión sobre la nueva información con el fin de identificar las vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.

- Defensas de malware: Controlar la instalación, difusión y ejecución de código malicioso en múltiples puntos de la entidad, al tiempo que se optimiza el uso de la automatización para permitir una rápida actualización de las defensas, la recopilación de datos y la acción correctiva.

- Aplicación de Software de Seguridad: Administrar el ciclo de vida de seguridad de todo el software in-house desarrollado y adquirido con el fin de prevenir, detectar y corregir las debilidades de seguridad.

- Control de Acceso Inalámbrico: Los procesos y las herramientas que se utilizan para realizar un seguimiento / control / evitar / corregir el uso de la seguridad de las redes inalámbricas de área local (LAN), puntos de acceso y sistemas de cliente inalámbrico.

- Capacidad de Recuperación de Datos: Los procesos y las herramientas utilizadas para respaldar adecuadamente la información crítica con una metodología probada para la recuperación oportuna de la misma.

- Capacitación y Entrenamiento en Seguridad: Para todos los roles funcionales de la organización (priorizando los de misión crítica para el negocio y su seguridad), identificar los conocimientos, destrezas y habilidades necesarias para apoyar la defensa de la empresa; desarrollar y ejecutar un plan integrado para evaluar, identificar las brechas, y remediar a través de programas de concienciación y capacitación.

- Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches: Establecer, implementar y gestionar activamente la configuración de seguridad de los dispositivos de infraestructura de red utilizando una rigurosa gestión de la configuración y cambiar el proceso de control con el fin de evitar que los atacantes exploten los servicios vulnerables.

- Limitación y Control de la Red de puertos, protocolos y servicios: Administrar el uso operacional continuo de puertos, protocolos y servicios en los dispositivos conectados en red con el fin de minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

- El uso controlado de privilegios administrativos: Identificar y planear los procesos y las herramientas para controlar las actividades de los administradores de servidores, aplicaciones, bases de datos y redes.

- Límites de Defensa: Detectar / evitar / corregir el flujo de información a transferir en las redes de los diferentes niveles de confianza con un enfoque en los datos que afectan la seguridad.

- Mantenimiento, Monitoreo y Análisis de registros de auditoría: Recoger, gestionar y analizar los registros de auditoría de eventos que podrían ayudar a detectar, comprender, o recuperarse de un ataque.

- Acceso controlado Basado en lo que necesita conocer: El acceso a los recursos y datos que se le otorguen a los usuarios deben partir de la pregunta: “Lo necesita conocer para su trabajo”.

- Monitoreo y Control de Cuenta: Gestionar activamente el ciclo de vida del sistema y de cuentas de aplicaciones desde su creación, el uso, la inactividad y la eliminación; con el fin de reducir al mínimo las oportunidades para que los atacantes se aprovechen de ellos.

- Protección De Datos: Los procesos y herramientas utilizados para prevenir la fuga de datos, mitigar los efectos de los datos filtrados, y garantizar la privacidad e integridad de la información sensible.

- Respuesta y Gestión de Incidentes: Proteger la información de la organización, así como su reputación, mediante el desarrollo y la implementación de una infraestructura de respuesta a incidentes (por ejemplo, los planes, los roles definidos, capacitación, comunicaciones, supervisión de gestión) para descubrir rápidamente un ataque y contener el daño y erradicar la causa raíz, y la restauración de la integridad de la red y sistemas.

- Ingeniería de red segura: Diseñar la seguridad de la información con base en las capas de protección que se deben activar en cada elemento de red para elevar la confianza del funcionamiento de los sistemas.

- Pruebas de Penetración y Ejercicios de respuesta: Evaluar de manera periódica la fortaleza general de las defensas de la entidad mediante la realización de ataques controlados a la infraestructura de TI simulando un ataque real.

6.6.3 Resultados. Los resultados de la gestión y operación de la seguridad se resumen en el diagrama de seguridad informática existente al cierre del proyecto fruto de las acciones correctivas y los proyectos de fortalecimiento de la seguridad emprendidos por la ANH. Ver figura 12.

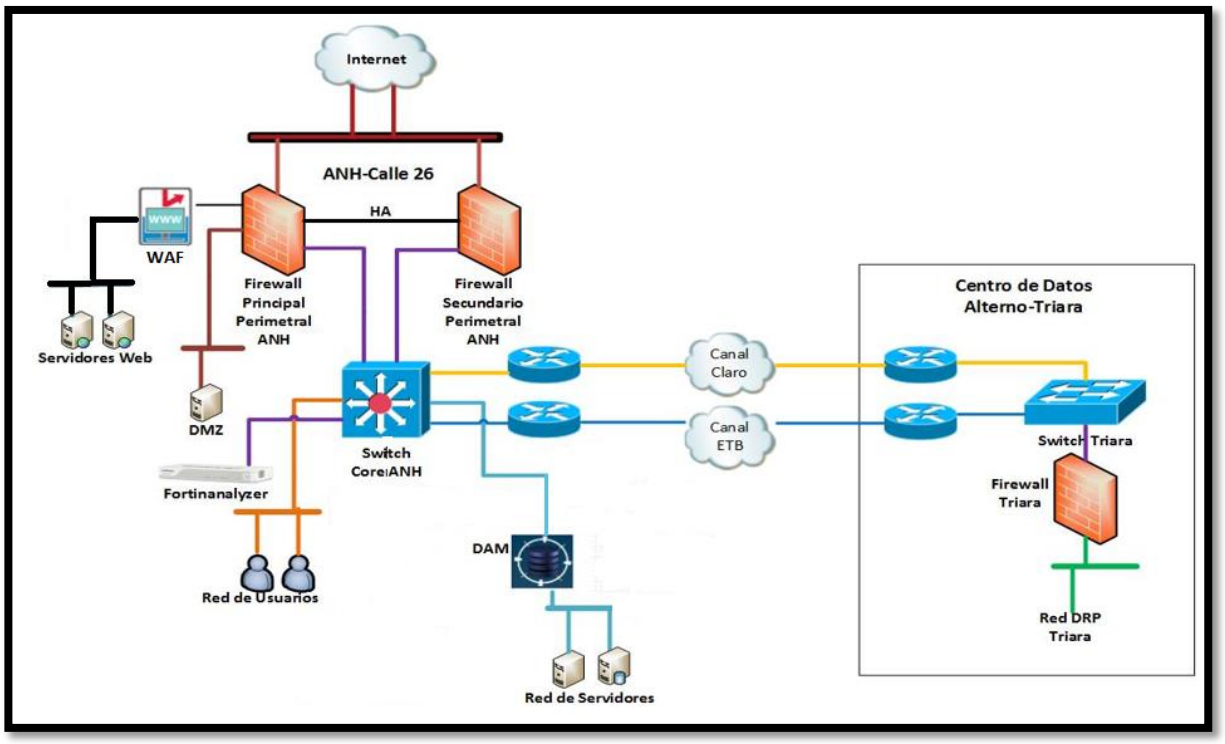
A continuación una relación de las principales características de seguridad de los diferentes dispositivos implementados en la ANH durante el proyecto:

Firewalls Calle 26 en Alta disponibilidad: El licenciamiento de los firewalls de Calle 26 fue renovado en hasta el 9 de Junio de 2015, la versión de firmware fue actualizada a la versión 5.0 build 3608 GA Patch 7 la cual cuenta con características de NGFW (NextGeneration Firewall) con soporte contratado a un tercero.

Actualmente las políticas y NATs asociados a las aplicaciones publicadas se encuentran definidos por puerto y protocolo y las políticas que se han configurado a nivel interno se encuentran depuradas. En cuanto a los perfiles de navegación, el perfil Internet Standard se restringió en las siguientes categorías:

PotentiallyLiable, Adult/Mature Content, BandwidthConsuming y Security Risk y subcategorías: Digital Postcards, Entertainment, Games, InstantMessaging, Personal Privacy, Personal Websites and Blogs, Social Networking y Web Chat.

Figura 11. Diagrama de seguridad al cierre del proyecto



Fuente: Autores

- El perfil Internet VIP se restringió en las siguientes categorías: Potentially Liable, Adult/Mature Content y Security Risk y subcategorías: File Sharing and Storage, Freeware and Software Downloads y Peer to peer File Sharing.

- Se eliminaron las rutas estáticas de redes directamente conectadas.

- Se configuraron grupos de usuarios para el manejo de perfiles VPNs SSL, de tal forma que el acceso de los proveedores queda limitado a los recursos internos de la ANH.

- Por último se realizaron pruebas satisfactorias de alta disponibilidad activo-pasivo.

Firewall CDA-Triara: El licenciamiento de este firewall fue renovado hasta el 9 de Junio de 2015, la versión de firmware fue actualizada a la versión 5.0 build 3608

GA Patch 7 la cual cuenta con características de NGFW (NextGeneration Firewall) y el soporte se encuentra contratado a un tercero.

- Se cuenta con conexión del canal del CAO (Centro Alterno de Operaciones), el cual tiene un ancho de banda de 6 MB y se utiliza en escenarios de contingencia en caso que los usuarios críticos de la ANH no puedan ingresar a las instalaciones físicas principales.

- Se encuentran configuradas las políticas necesarias para permitir acceso a los usuarios del CAO a la red servidores de Triara (172.20.xx.0/xx).

- Se cuenta con una conexión de Internet con un canal de 2 MB el cual se utiliza para el servicio de correo, conexión por VPN y navegación de los usuarios del CAO en escenarios de contingencia.

- Las políticas y NATs necesarios para permitir navegación a los usuarios del CAO, publicar el servicio de correo y de VPN se encuentran configuradas.

Fortianalyzer: El licenciamiento de este appliance fue renovado en el mes de Noviembre de 2013 hasta el 9 de Junio de 2015, la versión de firmware se actualizo a la versión v5.0.10-build 0365 150129 (GA). El soporte se encuentra contratado con un tercero.

- Actualmente se utilizan los reportes que se pueden generar mediante esta herramienta, en especial los reportes de VPN y Web Usage para sacar estadísticas para los informes de gestión mensual.

Antispam Calle 26: Se instaló la licencia de OSE MailSecure, la cual tiene vigencia hasta el 10 de Agosto de 2015, se extrajo el backup a una carpeta compartida y se cambió la contraseña por defecto del usuario user_sys.

Por otra parte se realizó migración de la consola antispam a un nuevo appliance y se ejecutó mantenimiento a nivel lógico por parte del proveedor, se realiza entrenamiento continuo con el proveedor sobre el algoritmo de detección de SPAM.

Antispam CDA – Triara: Se instaló la licencia de OSE MailSecure, la cual tiene vigencia hasta el 10 de Agosto de 2015, se extrajo el backup a una carpeta compartida y se cambió la contraseña por defecto del usuario user_sys.

Por otra parte se realizó configuración para que este equipo filtre correo entrante en escenarios de contingencia, y se realizaron pruebas exitosas en los simulacros DRP.

Consola EPO: Se realizó despliegue de agente de McAfee, antivirus y agente DLP a las estaciones de trabajo y servidores de la ANH.

- Se configuro regla de bloqueo de USB y se aplicó a equipos de contratistas de manera paulatina para dar cumplimiento a la política de terceros.

- Se eliminaron los equipos que llevaban un tiempo considerable sin comunicarse con la consola EPO y los que estaban en estado Unmanaged.

- Por otra se actualizo la versión de software de la consola EPO a la versión 5.1.1 Build 509 y la versión de DLP a la versión 9.3.300.31.

WAF (Web Application Firewall): El Firewall de aplicaciones marca Fortinet, referencia Fortiweb 3000D se encuentra operativo y en funcionamiento, se configuraron las aplicaciones en modo bloqueo después de un periodo de monitoreo.

Se configuraron aplicaciones adicionales a lo largo del proyecto y se eliminaron las aplicaciones que no se encuentran operativas. Quedaron 14 aplicaciones en modo producción (bloqueo) y 6 en modo monitoreo (observación):

DAM (DatabaseActivityMonitoring): La solución DAM de McAfee está en etapa de afinamiento, el proveedor se encuentra configurando las alertas con la información suministrada por el Administrador de las bases de datos para definir cuales eventos son falsos positivos y cuales son relevantes para definir en qué casos se debe generar alerta.

MVM – McAfee Vulnerability Manager: La herramienta se entregó operativa y en producción. Se deja actualizada con las últimas firmas de ataques y parches de sistema operativo a 27 de Marzo de 2015. Se actualiza el inventario de activos y la clasificación de criticidad de los mismos a marzo 31 de 2015.

Se atendieron las visitas trimestrales de mantenimiento del proveedor en las siguientes fechas:

- Septiembre 4 de 2014

- Noviembre 18 de 2014

- Febrero 12 de 2015 (Entrega informe Análisis de Vulnerabilidades)

SIEM – Sistema de Correlación de eventos: La herramienta se encuentra operativa y en producción. Durante la ejecución del proyecto se realizó la administración y mantenimiento para incluir en ella equipos que cambiaban de

versión, como por ejemplo el firewall Fortigate que al ser actualizado perdió conexión con la consola y fue necesario reconfigurarlo en el SIEM, al igual que las contraseñas de dominio para tener acceso a los servidores Windows incluidos en la consola. Para realizar estas labores se contó con el soporte del proveedor en visitas mensuales de soporte preventivo y correctivo, las cuales se realizaron en las siguientes fechas:

- Julio 02 de 2013
- Agosto 15 de 2013
- Agosto 28 de 2013
- Octubre 2 de 2013
- Octubre 23 de 2013
- Noviembre 27 de 2013
- Diciembre 23 de 2013
- Enero 22 de 2014
- Febrero 26 de 2014
- Marzo 18 de 2014

Gestión de Incidentes (RSA Archer IM): Sobre esta herramienta se realizó la documentación de todos los incidentes de seguridad presentados durante la ejecución del proyecto, configurando y probando el funcionamiento de correcto de las alertas vía correo electrónico.

Se realizó manual de usuario, matriz de roles y una charla de capacitación sobre el funcionamiento de la herramienta y la gestión de incidentes con todo el grupo de especialistas de infraestructura.

6.7 GESTIÓN DE VULNERABILIDADES TÉCNICAS

6.7.1 Análisis de vulnerabilidades de red. Se realizaron de forma programada para sobre servidores Windows, Linux y VMWare, Switches y Estaciones de trabajo. En el 2014 se realizaron 3 análisis en los siguientes meses:

- Marzo de 2014
- Julio de 2014
- Diciembre de 2014

El análisis realizado en diciembre, se ejecuta con el apoyo del proveedor de la herramienta MVM usada para Gestión de Vulnerabilidades. Existen algunas aplicaciones Legacy que por requerimientos del negocio siguen activas aunque no cuentan con soporte, por esto no han sido actualizados ni sus sistemas operativos y generan gran número de vulnerabilidades altas que aparecen repetidamente en todos los análisis de vulnerabilidades realizados.

Como respuesta a esto, se realizó una reunión el 18 de septiembre de 2014, documentada en el Acta No. 16, donde se presentó el plan de remediación clasificando los servidores en tres grupos:

- Servidores 100% administrados por el outsourcing de TI.
- Servidores de Aplicaciones de terceros que cuentan con algún tipo de soporte.
- Servidores de Aplicaciones de terceros que no cuentan con ningún tipo de soporte.
- Servidores con aplicaciones desarrolladas por la ANH.

6.7.2 Análisis de vulnerabilidades de aplicaciones. Se realizaron en las siguientes fechas de acuerdo con las solicitudes recibidas, y por aplicaciones antes de su salida a producción:

Cuadro 20. Programación de análisis de vulnerabilidades de aplicaciones

Aplicación	Fecha
Chat	9 de diciembre de 2014
Dataroom	20 de enero de 2014
FileDataroom	31 de enero de 2014
Geovisor y Geoportal	23 de enero de 2014
MIGEP	19 de Junio de 2014
Retest MIGEP	3 de Julio de 2014

Cuadro 18. (Continuación)

Aplicación	Fecha
Segundo Retest MIGEP	10 de Julio de 2014
Schlumberger: SIR, SIP e IDP	14 de noviembre de 2014
SSCH Seguimiento y Control Contratos Hidrocarburos	15 de mayo de 2014

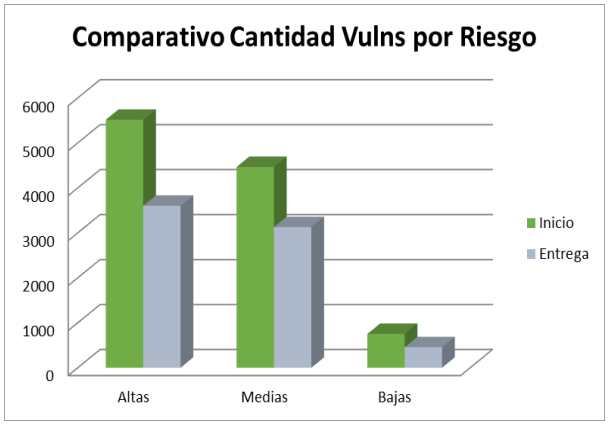
Fuente: Autores

6.7.3 Pruebas de Hacking Ético. Adicionalmente, en Septiembre se realizaron Pruebas de Hacking ético, sobre los siguientes servidores:

- 172.20.xx.xx – SMAILV
- 172.20.xx.xx – SMAILDRP
- SVANH-DB
- Sistema Integrado de Pozos
- SGI Sungemini

Plan de remediación: Como se mencionó anteriormente, en respuesta a los resultados repetitivos de los análisis de vulnerabilidades, donde el gran porcentaje de vulnerabilidades se debía a la ausencia de parches y actualizaciones, se realizó en Septiembre de 2014, el Plan de remediación el cual contiene una Política de Actualización mensual de plataforma.

Figura 12. Evolución en la gestión de vulnerabilidades técnicas



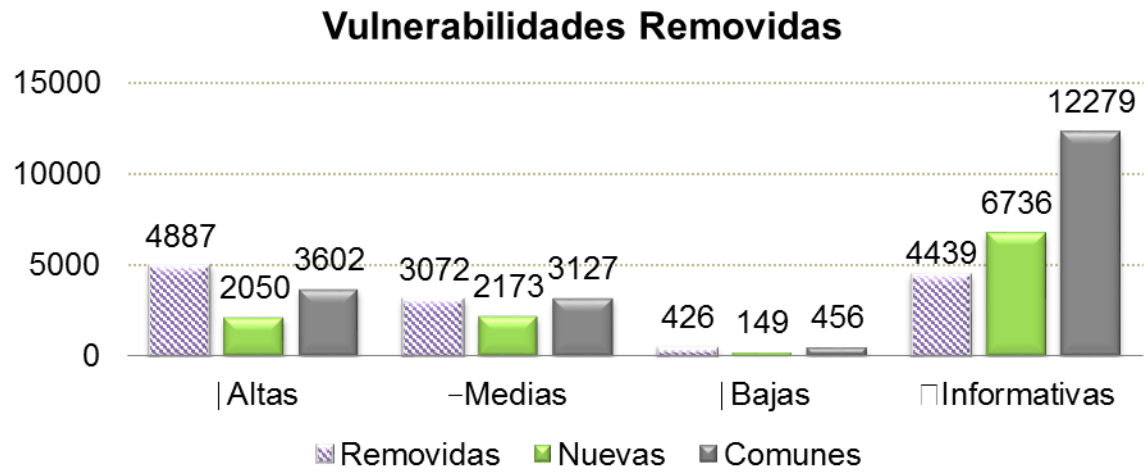
Fuente: Autores

En la figura 13 podemos observar un comparativo entre el último análisis de vulnerabilidades realizado inicio del proyecto y el último análisis de vulnerabilidades realizado, es decir el estado de la entrega, donde se observa que la cantidad de vulnerabilidades disminuyó notablemente. Ver figura 13.

Es importante tener en cuenta que a nivel de vulnerabilidades, las cantidades no es el único indicador de gestión, el nivel de vulnerabilidades removidas en un buen indicador de la gestión realizada.

En el siguiente gráfico se puede observar, que la cantidad de vulnerabilidades removidas es alta y es mayor que la cantidad de vulnerabilidades nuevas que aparecieron, y que la cantidad de vulnerabilidades que permanecen. Ver figura 14

Figura 13. Vulnerabilidades Removidas



Fuente: Autores

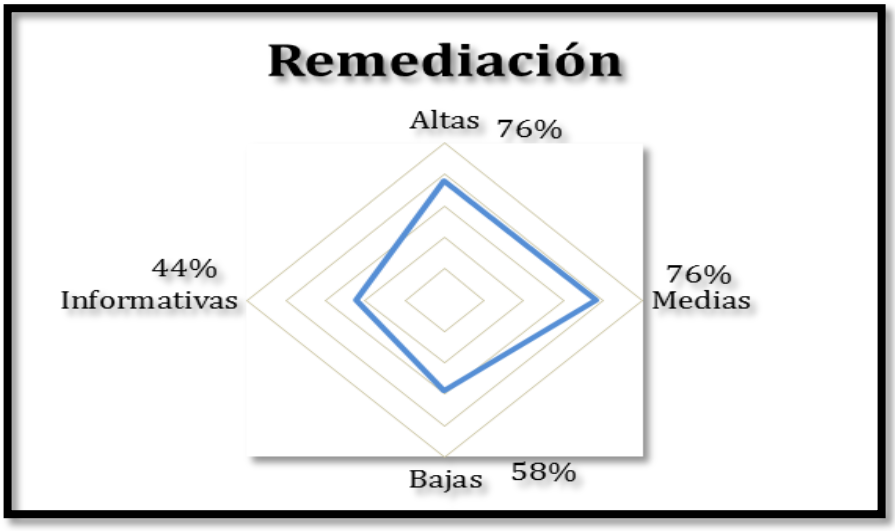
Con esto podemos concluir que el objetivo propuesto con la política mensual de actualización de plataforma, aprobado en Septiembre de 2014, fue logrado, al obtener un 76% de remediación en las vulnerabilidades altas, 76% en las medias y 58% en las bajas. Ver figura 15.

Los mayores niveles de remediación se dieron en estaciones de trabajo, con la puesta en producción del servidor de actualizaciones WSUS, y en Servidores Windows por la gestión de actualizaciones manuales realizadas por el especialista en Administración de Servidores Windows.

6.7.4 Gestión de Incidentes de seguridad informática. Se diseñó e implemento el procedimiento de gestión de incidentes de seguridad informática. Durante el proyecto se registraron 5 casos que ameritaron investigación, seguimiento y cierre, incluyendo defacement de la página web e imposibilidad de generar reportes de

las herramientas de seguridad por falta de espacio para el almacenamiento de los mismos.

Figura 14. Porcentajes de remediación logrados



Fuente: Autores

6.7.5 Otras Acciones Emprendidas. Dentro del programa de seguridad de la información se realizaron las siguientes tareas, claves para mejorar la protección de la información:

Seguridad Informática

- En la consola EPO se configuró una tarea para enviar por correo top 10 diario de detecciones y top 10 diario de usuarios con más detecciones, con el fin de identificar de manera más fácil los equipos que representan una amenaza para la seguridad de la red de la ANH.

- Apoyo en la implementación del Firewall de aplicaciones web (WAF) y de la herramienta para monitoreo de bases de datos (DAM) adquiridos por la ANH para proteger las aplicaciones web de ataques internos y externos y para facilitar la visibilidad de las actividades que se realizan sobre las bases de datos con el fin de construir políticas que generen alertas cuando se detecte tráfico que coincida con patrones de ataque.

- La integración del Directorio Activo y el Firewall, con el fin de evitar el uso de los agentes FSSO y de esta forma minimizar los inconvenientes que se presentan algunas veces con la navegación de algunas estaciones de trabajo.

- Instalar los certificados digitales de las siguientes aplicaciones: OWA, OWA DRP, Sistema Integrado de Reservas y Ronda Colombia 2012.

- Documentación de la topología física de las conexiones del firewall, direccionamiento público, de los NATs y de la red.

- Apoyo para puesta en producción del sistema de videoconferencia.

- Depuración de reglas y NATs configurados en el firewall para servicios publicados.

- Despliegue en estaciones de trabajo que no tenían instalado el agente de McAfee, el antivirus y el DLP.

- Se realizaron pruebas de filtrado de correo entrante en Triara con el fin de evitar el ingreso de SPAM a las bandejas de entrada en escenarios de contingencia, se determinó que el algoritmo de detección no es eficiente y requiere afinamiento.

- Aseguramiento para publicación de las siguientes aplicaciones: Geovisor, Geoportal, Dataroom, File Dataroom y GeovisorDataroom.

- Prueba de concepto con solución de gobierno de datos para control de acceso a la información.

- Depuración de conexión por VPN de proveedores.

- Depuración de reglas de acceso por VPN de funcionarios de la ANH.

- Afinamiento de los perfiles de filtrado web Internet Standard e Internet VIP, el cual mejoro considerablemente el consumo de ancho de banda del canal de internet.

- Configuración de Optenet de Centro de Datos Alterno para filtrado de correo.

- Configuración de cuentas para conexión por VPN en Firewall de Triara.

- Apoyo para instalación de certificados SSL con validación extendida, adquiridos por la ANH en servidores de aplicaciones web, hasta el momento se han instalado los siguientes certificados: Sitio Web, SUIME, Modulo PQRs, IDP, Geoportal, Geovisor, Videoconferencia, Dataroom, File Dataroom y SIP.

- Migración de canales de Internet con ETB con el nuevo proveedor IFX, publicación servicios externos con nuevo direccionamiento y configuración de VPN principal y de contingencia.

- Configuración y re direccionamiento de HTTP a HTTPS para las siguientes aplicaciones: Sitio Web, Suime, Sigeco PQR, Geoportal y Videoconferencias.

- Se realizó afinamiento de reglas internas en los firewalls de Calle 26 configurados en HA.

Seguridad de la Información

- Análisis de los catálogos de servicios y de información producidos por PWC en el marco del proyecto PETI que adelanta la ANH.

- Entrega de las estadísticas del uso del almacenamiento y el análisis de datos del Banco de datos de información petrolera.

- Entrega de políticas de prevención de fuga de información, seguridad de terceros, disposición de activos de información.

- Evaluación y participación en la entrega del sistema MIGEP con la línea base inicial del BIP definida.

- Informe BIA, DRP, inventario del EPIS, Escenarios de desastre, Plan de recuperación de desastres y apagado Centro de Datos Principal.

- Traslado de los bunker del centro de cómputo alterno a una única ubicación geográfica en Triara.

- Soporte a la operación durante los apagados del centro de cómputo principal causados por cortes de energía abruptos o programados por Codensa.

- Desarrollo de campañas en seguridad de la información.

- Informe de iniciativas de seguridad y DRP para el sector minas y energía.

- Actualización de la matriz de riesgos de disponibilidad.

- Sustentación del informe de línea base del EPIS a la Contraloría.
- Análisis y revisión del copiado del nodo ISILON de LITOTECA.
- Presentación de recomendaciones para el fortalecimiento del DRP de la ANH.
- Participación en las reuniones de ciber-seguridad en representación de la ANH
- Revisión y ajuste de las recomendaciones de estrategias de recuperación.
- Propuesta de árbol de comunicaciones del DRP.
- Trabajo con la Vicepresidencia Técnica para la organización del proyecto de entrega del Banco de Información Petrolera al Servicio Geológico Colombiano.
- Desarrollo de las políticas y procedimientos de seguridad de la información bajo ISO 27001:2013 y el modelo de Gobierno en Línea (GEL).

6.8 EVALUACION DE PRESENCIA DE APT´s EN LA ANH

Durante el desarrollo del proyecto, en una conferencia de seguridad, uno de los proveedores de herramientas para prevención y contención de las amenazas avanzadas persistentes (APT´s) hizo la siguiente afirmación: *"Por más seguridad que tenga su empresa, ya tiene APT´s instaladas"*. Esta afirmación generó inquietudes en el equipo de trabajo pues hasta ese momento, MINTIC y entidades del sector minas y energía de Colombia tuvieron oportunidad de conocer y evaluar el programa de gestión de seguridad de la ANH y la concluyéndose que este era uno de los modelos más maduros a nivel de entidades de gobierno, lo cual generó la sensación de seguridad razonable. Sin embargo se decidió emprender un plan de trabajo para identificar la presencia de APT´s en la infraestructura de la entidad.

El plan de trabajo se dividió en tres fases: Identificación de herramientas de protección APT´s existentes en el mercado, realización de pruebas de concepto y análisis de resultados.

6.8.1 Identificación de Herramientas de protección APT´s. Se buscaron soluciones para APT y se indagaron las características de cuatro herramientas:

- Verint
- FireEye

- Iboss

- TippingPoint

Threat Protection System (TPS) de Verint: Es un sistema de protección contra amenazas cibernéticas avanzadas creado como una solución adaptable al tamaño de las organizaciones, al tamaño y distribución de la red que se integra fácilmente con los activos TI y seguridad existente. Fue diseñado con el propósito de prevenir ataques cibernéticos avanzados actuando en cada etapa del ciclo de ataque. El propósito principal es ayudar a detectar, investigar, remediar ataques avanzados empleando un conjunto de características pre-integradas para detectar y detener los ataques en todas sus etapas.

- Motores de detección especializados: TPS monitorea el tráfico de web y email, tráfico interno y puntos finales, detectando automáticamente ataques invisibles a las defensas tradicionales. Mediante los motores de detección avanzados enfocados en la etapa específica del ciclo de ataque, se detectan ataques dirigidos de día cero y determinar los puntos finales infectados. El análisis heurístico de archivo estático y análisis profundo de archivo dinámico detectan malware conocido y desconocido. El análisis multidimensional a través de redes y puntos finales revela movimiento lateral del ataque dentro del entorno, mientras un motor especializado detecta las tentativas del malware para evitar la detección.

- Fusión y priorización de alertas automatizadas: Mediante algoritmos especializados se filtra el ruido y se identifican riesgos potenciales, sin la necesidad de implementar cientos de reglas. Las funcionalidades de fusión y priorización trabajan en sincronismo para combinar alertas, metadatos e inteligencia en incidentes acelerando el tiempo de detección y asegurando que los investigadores se enfoquen en los riesgos más altos y urgentes para la organización. El análisis forense automatizado y dinámico adapta la trayectoria de la investigación sobre la marcha mientras los hallazgos son procesados, tales como elevar el nivel de sensibilidad del motor para recolectar más evidencias relevantes.

- Investigación, análisis forense y análisis unificados: El entorno de investigación pre-integrado permite al analista obtener una visibilidad completa dentro de un ataque. Combina poderosas herramientas de red, punto final y registro forense para responder preguntas que importan en un ataque como son: quien ataco, cuando, como, el ataque continua y como evitar ocurrencias futuras. Teniendo esta parte de la investigación automatizada los analistas ahorran tiempo y ganan agilidad al responder a amenazas y ataques cibernéticos nuevos.

- Reportes: Los hallazgos son presentados en informes intuitivos y mapas de ataque visuales que muestran el flujo del ataque según cronogramas, geografía y activos de TI comprometidos. Herramientas forenses multidimensionales reiterativas buscan tanto hacia adelante como hacia atrás en el tiempo para construir un cuadro de inteligencia comprensivo. Esto permite a los analistas verificar si se presentaron ataques previos similares, estar atentos a posibles ataques futuros con atributos parecidos y asegurar que no haya malware adicional desplegándose a través de la red.

- Inteligencia accionable para remediación proactiva: TPS crea automáticamente inteligencia accionable que puede ser usada para eliminar el malware detectado en las redes y en los puntos infectados. La protección contra amenazas futuras se logra mediante la actualización de las herramientas de seguridad con descubrimientos clave para evitar ataques repetitivos. Adicional a los propios hallazgos se recibe la actualización de información sobre las amenazas globales proveniente del plantel de investigación de Verint y de otras fuentes.

FireEye: Es una solución integrada orientada a detener los ataques a través de las etapas de su ciclo de vida, desde la explotación a la ex-filtración. Su principal objetivo es proteger contra las amenazas de próxima generación.

- Utiliza una plataforma de tecnología patentada denominada Virtual Execution. FireEye es referencia en la detección de amenazas de próxima generación, como los ataques APTs o los de día cero que eluden las defensas tradicionales, tales como cortafuegos, IPS, antivirus, pasarelas de anti-spam y comprometen las redes organizacionales.

- Las soluciones de FireEye completan los sistemas de defensa tradicionales como los cortafuegos o los IPSs, las soluciones antivirus y las pasarelas web que no pueden detener las amenazas avanzadas.Medianteappliances de FireEye se refuerza la seguridad de los equipos conectados a la red de la empresa, evita la perdida de datos, mantiene centralizada la gestión, evidenciando la actividad de malware furtivos que esquivan los sistemas clásicos de seguridad, pasan por encima de los filtros existentes y evitan los detectores de anomalías. Mediante esta detección FireEye evita el contagio a más puestos de trabajo.

Iboss Security: Esta solución promueve las siguientes características:

- Filtrado web: El Filtro Web Iboss SWG es una solución completa pero fácil de usar que escanea a través de SSL/HTTPS para proteger información sensible, controla los recursos de red mediante funciones de gestión de ancho de banda, regula la forma en que se accede al contenido de redes sociales, identifica amenazas y reporta tráfico. Además, permite máximo control y flexibilidad, gracias a sus avanzadas políticas de filtrado que se pueden configurar según grupos de usuarios.

- Para abordar la “nueva Web,” el Filtro Web Iboss SWG protege todos los aspectos del tráfico de Internet, incluyendo el filtrado de web, acceso SSL, aplicaciones, límite/ de ancho de banda/ calidad de servicio (QoS), seguridad móvil dentro y fuera de las instalaciones, y herramientas de gestión de BYOD. Esta suite de seguridad integral está diseñada para proteger todos los aspectos del tráfico alámbrico e inalámbrico, tanto dentro como fuera de las instalaciones. Mientras que los filtros web tradicionales abordan el acceso web con un enfoque de "bueno/malo", el Filtro Web IbossSWGs se centra en la obtención de tecnología en la organización, incluso si los usuarios acceden a la red a través de una PC tradicional o un BYOD o desde un lugar fuera de las instalaciones.

- El filtro WEB Iboss SWG combina: Aplicación HTTPS, WEB 2.0: Web 2.0 introdujo la necesidad de proteger el tráfico más allá de los Puertos estándar 80 y 443 puesto que las nuevas aplicaciones como torrents, anonimizadores, y aplicaciones de chat como Yahoo y Google Chat deben utilizar puertos no estándar para la comunicación. Asegurar estos puertos garantiza la conformidad de la red y reduce la exposición a amenazas mientras que hace que se cumplan las políticas de uso aceptable (AUP) de la organización.

Tipping Point Advanced Threat Appliance: La tecnología Tipping Point Advanced Threat Appliance de HP supervisa el malware que se ejecuta en un entorno de espacio aislado seguro. Mediante la detección se identifica el comportamiento sospechoso, aísla el equipo infectado evitando la propagación lateral. Sus principales características son:

- Espacio aislado personalizado: Permite la configuración de los sistemas de detección para detectar ataques dirigidos que amenazan la red.

- Análisis forenses de ataques: Mediante motores de detección especializados, reglas de detección y espacio de aislamiento personalizado se pueden detectar todos los aspectos de una amenaza.

- Amplia detección de sistemas: Permite la detección de amenazas en la red independiente del sistema operativo.

- Análisis de adjuntos de correo electrónico: Utilizando motores de detección múltiples en espacios aislados, examina los datos adjuntos en un correo electrónico, incluyendo ejecutables de Windows, Office, pdf, zip entre otros. Así mismo permite:

- Detección de puntos vulnerables en documentos

- Análisis de URLs incrustadas

- Inteligencia de contraseñas

6.8.2 Comparación de las herramientas de protección APT. Las APT se caracterizan por reconocer y adaptarse al entorno del objetivo atacado, luego de introducirse sin ser detectadas en sistemas vulnerables mediante técnicas avanzadas de ingeniería social o valiéndose de ataques conocidos que atacan el recurso humano de la organización crean una puerta trasera en la red vulnerada, escalan accesos hacia sistemas informáticos internos y privilegios valiéndose de la instalación furtiva de otras aplicaciones o herramientas malintencionadas.

En definitiva este nivel de adaptación logrado por las APT requiere de tecnologías de defensa no cubiertas por los sistemas de defensa convencionales. De acuerdo a la teoría estas herramientas deben proveer soluciones que permitan detectar, prevenir, analizar y resolver los ataques avanzados optimizando los tiempos de detección y solución. Las fases de respuesta de estas herramientas responden a las fases de infección que caracterizan las amenazas avanzadas: Estudio, infección, propagación y explotación.

A modo de resumen se incluye un comparativo de las herramientas APT´s analizadas con la información relevada.

Cuadro 21. Programación de análisis de vulnerabilidades de aplicaciones

	Detectar	Prevenir	Analizar	Resolver
Iboss	●			
Tipping Point	●	●	●	●
FireEye	●	●	●	●
Verint TPS	●	●	●	●

Autor: Propio de proyecto

6.8.3 Realización de Pruebas de Concepto (POC). Se invitó a los diferentes proveedores a realizar una prueba de concepto para evaluar sus herramientas y recomendar a la entidad la implementación de este tipo de controles. Dos proveedores atendieron la invitación: FireEye y Iboss. Puesto que estas PoC requieren ventanas para su implementación se decidió iniciar con FireEye y finalizada esta se realizaría la de Iboss.

La planeación y realización de la prueba de FireEye se llevó a cabo con éxito. Iboss se planeó pero tuvo que competir con otras ventanas de mantenimiento y operación de la infraestructura lo que obligo a su postergación y finalmente no se pudo llevar a cabo dentro de la ejecución del proyecto.

Prueba de concepto de FireEye: Las amenazas persistentes avanzadas (APT), son la preocupación de los profesionales de seguridad de TI a nivel mundial. Esta prueba de concepto pretende dar a conocer el funcionamiento de la herramienta FireEye, y el diagnostico preliminar que permitá generar a partir de las pruebas realizadas sobre la infraestructura de la ANH.

Reporte de la herramienta FireEye: Las amenazas avanzadas y persistentes siguen evolucionando y usan unos exploits de programas malintencionados para esquivar la seguridad tradicional. FireEye es un appliance que ayuda a reforzar la seguridad en los puestos de trabajo conectados a la red de una empresa y permite a los responsables de seguridad de TI mantener el control de estos, destapando la actividad del malware avanzado. Este tipo de malware, tienden a ser bastante silenciosos porque pueden evadir los sistemas de seguridad.

A pesar que la ANH, tiene bastantes sistemas de seguridad y en un nivel de implementación alto, no está exento de las amenazas, toda vez que la herramienta detecto que la infraestructura interna de la organización está infectada con el siguiente malware.

BotConficker: Es un gusano informático que ataca sistemas operativos Windows. El gusano tiende a propagarse por medio de desbordamiento de buffer de algunos servicios Windows. Una vez infectado el computador, este gusano desactiva otros servicios Windows tales como: Windows AutomaticUpdates, Windows defender, Windows Error Reporting. Luego, a través de manera remota, se le puede dar órdenes al programa para propagarse una vez este recolecte todos los datos del usuario.

Host afectado: 192.xxx.xx.xx

Bloqueo de URLs:

http://216.66.xx.xxx/search?q=0
http://38.102.xxx.xx/search?q=0
http://221.8.xx.xx/search?q=0
http://149.93.xx.xxx/search?q=0

http://195.22.xx.xxx/search?q=0
http://195.22.xx.xxx/search?q=0

Malware ZerodayCallback: Está clasificado como malware, el cual tiene como objetivo infectar una máquina para así realizar función de Botnet. El objetivo de este tipo de malware, tiende a ser el robo de información o uso ilegal para no ser detectados en la red, y así generar ataques que permitan suplantar el origen.

Hosts afectados: 192.xxx.xx.xx, 192.xxx.xx.xx

Bloqueo de IP:

23.21.xxx.xxx A la red LAN y la red del EPIS

InfoStealerGeneric: Es una amenaza muy peligrosa, que fue desarrollada por varios hackers remotos con el fin de dañar las computadoras completamente. Realiza un seguimiento de las pulsaciones de teclado, toda la aplicación utilizada, todo el historial de navegación, etc. Se puede disminuir el rendimiento del sistema y lleva a la parada brusca del ordenador. Infostealer está generalmente presente en el lugar oculto en el disco duro del sistema. Puede bloquear el equipo y en el peor de los casos exige dinero para recuperar el problema. Cambia la página de inicio y redirige las búsquedas completas de los sitios Web maliciosos. Tiene capacidad para entrar automáticamente en el sistema del usuario sin el consentimiento del mismo.

Hosts afectados:192.xxx.xx.xxx

Virus Sality AT:Sality es una clasificación que se le dio a una familia de malware que tiende a infectar sistemas de archivos Windows. Este tipo de malware puede comunicarse sobre una red P2P para el propósito de esparcir spam, comunicaciones proxy, extracción de datos sensibles y/o coordinar password cracking distribuido. Este tipo de malware es considerado como una de los más formidables.

Host afectados: 192.xxx.xx.xx

Bloqueo de URL:

MalwareBinary: Es una clasificación para ciertos tipos de malware, que son adquiridos por descargas a través de internet. El usuario se infecta a partir de la ejecución de programas que no son lo que aparentan. Al igual que las amenazas

anteriores, son usados para alterar registros de Windows, robo de información sensible.

Host afectados: 192.xxx.xx.xxx, 192.xxx.xxx.xxx

Backdoor APT 9002: Es una pieza de malware que se tiende a ser inyectada a través de vulnerabilidades de Internet Explorer. Su característica principal, es que el malware es escrito directamente en memoria, es decir que no se aloja en la máquina de forma permanente. Al tener esta característica, trata de cumplir su objetivo, antes de realizar el apagado o reinicio del host. Esto indica que en algunos casos el malware no permite el apagado normal del computador (o mejor, toca forzar el apagado). La ventaja para el atacante, es que en caso de querer examinar el host de la víctima (como análisis forense), si la maquina se apaga no se podrá encontrar evidencia alguna de que hubiese existido este malware.

Host afectados: 192.xxx.xx.xx, 192.xxx.xx.xxx, 192.xxx.xx.xxx

Se presentó para investigación por parte de Fábrica.

Malware.Archive: Esta detección por parte de la herramienta, indica que uno o más archivos sobre la victima están infectados, o bien es software malicioso (malware). Puede ser un malware polimórfico, que tiende a sobre-escribirse a sí mismo para no ser detectado.

Host afectados: 192.xxx.xx.xxx

Host Destino: 192.xxx.xxx.xxx

TrojanGeneric: Este malware permite el acceso remoto a cualquier máquina que está infectada. Es el clásico Troyano, pero éste no se propaga de forma automática. Generalmente se adquiere por descargas a través de internet

Source IP: 192.xxx.xx.xxx

Destination IP: 192.xxx.xx.x

HTTP REQUEST EOH: Aunque la herramienta no muestra información concerniente a este tipo de amenaza, puede ser un falso positivo que se basa en un análisis de cabeceras de paquetes TCP. Snort es una herramienta que sirve para la implementación de IDS, el cual tiende a arrojar muchas alarmas

relacionadas con este tipo de paquetes, porque determina que está evadiendo de alguna forma la seguridad por técnicas de encode o decode http.

Source IP: 192.xxx.xx.xxx

Destination IP: 192.xxx.xxx.xxx

Trojan.Generic.DNS: Este troyano basicamente fuerza al sistema a usar servidores DNS, para direccionar a la victima a paginas de atacantes que de alguna manera pretenden interceptar, fabricar o manipular datos propios del usuario.

Source IP: 192.xxx.xx.xxx

Destination IP: 114.112.xx.xxx (http://srtj.pctutu.net/)

Backdoor.Xtrat.A:Es un malware que se caracteriza por otorgar acceso remoto al atacante. El uso principal de esta herramienta, es para el robo de información sensible del usuario.

Source IP: 192.xxx.xx.xxx

Destination IP:

181.136.x.xx (http://solaris1986.no-ip.biz:3000/19921782.functions)
181.136.xx.x (http://pallares123.dvrdns.org:4050/1234567890.functions)

Win.Adware.Toggle: Este tipo de malware tiende a afectar la navegacion del browser. Utiliza adware, para mostrar o realizar spam de adwares sobres la victima. Algunos tipos de este malware, instalan barras o complementos de “ayuda” sobre el browser, causando que la navegacion o funcionamiento de la maquina se vean estropeados.

Source IP: 192.xxx.xx.xxx, 192.xxx.xx.xxx

Destination IP: 54.230.xx.xxx, 54.230.xx.xxx

6.8.4 Análisis de Resultados. La ANH cuenta con un equipo de seguridad bastante robusto, que en parte le permite defenderse de ataques externos. En la mayoría de los casos los grandes problemas de las organizaciones a nivel de seguridad de la información, tienden a ser vulnerados desde el interior de la compañía (desde empleados inconformes hasta espionaje industrial).

- Se encontró presencia de malware avanzado dentro de la ANH, lo que es indicativo que los elementos de protección actualmente implementados por la organización no han sido suficientes para evitar la propagación y poniendo de presente que se requieren medidas de protección adicionales que pueden ser valoradas desde el fortalecimiento de las políticas, la configuración de las herramientas actuales hasta la implementación de una herramienta de protección contra amenazas de nueva generación.

- Dado que las amenazas ya se encuentran en los equipos es probable que la infección se haya generado por falta de implementación y fortalecimiento de políticas que restrinjan el uso inadecuado de los equipos así como de la instalación de equipos de cómputo y dispositivos electrónicos de los funcionarios o de las terceras partes.

- Es necesario realizar un seguimiento a todos los usuarios de la navegación propia de la ANH para poder determinar cada una de las actividades que están realizando en horas laborales, y verificar el origen (si se puede) de la adquisición de malware en los equipos. Adicionalmente clasificar la sensibilidad de los activos, para así poder cuantificar las pérdidas monetarias que estos puedan causar

- Para evitar la instalación de este tipo de software malicioso, se sugiere limitar el permiso de los usuarios en cada una de las estaciones. Esto ayuda a mitigar la ejecución de malware, ya que estos no deberían ser ejecutados sin el permiso del administrador de TI.

- Si bien la prueba de concepto mediante FireEye no evidenció que mediante el malware se hubiese fugado información de la organización, la prueba demostró que integrar este tipo de herramientas en la estrategia de defensa en profundidad le suma fortaleza adicional de prevenir y detectar el malware que ha sobrepasado con éxito defensas perimetrales de la red y que de acuerdo a las características avanzadas de las APT pueden ser puntos iniciales para vulnerar la organización.

6.8.5 Como Enfrentar las Amenazas Persistentes Avanzadas (APT´s). La estrategia de defensa aplicada actualmente en la mayoría de las organizaciones está basada en la implementación de múltiples sistemas de protección desintegrados que no fueron diseñados para realizar investigaciones en profundidad. Por su parte los ataques cibernéticos avanzados se valen de operaciones meticulosas e integradas que incluyen un conjunto definido de técnicas de reconocimiento, infiltración y robo de datos teniendo la posibilidad de invertir altos recursos en el propósito de afectar el objetivo.

Mientras el grupo de seguridad se puede enfrentar infinidad de alertas generadas continuamente, no tienen la posibilidad de investigar a fondo o correlacionar los datos encontrados en cada sistema. De acuerdo a lo anterior el criterio de seguridad frente a las amenazas persistentes avanzadas es obsoleto y continuamente fallido especialmente por la capacidad que tienen los atacantes para adaptarse a estos esquemas de seguridad.

La implementación de sistemas de seguridad y análisis automatizados e integrados permiten a los analistas de seguridad eliminar lo superficial y orientarse a los ataques que realmente son importantes, la aplicación de estas herramientas reducen el tiempo de detección, aumentan la eficiencia y con ello detener los ataques y reforzar la seguridad contra posibles ataques futuros**.**

Para establecer una estrategia de defensa más robusta frente a las APT´s, se recomienda considerar los siguientes elementos:

- El malware realmente ya está en la organización
- Es necesario re-imaginar la seguridad
- Se requiere un giro hacia la seguridad adaptativa
- Se requiere una defensa integrada End To End
- Reconocer que la defensa en profundidad no es suficiente

El Malware Realmente ya Está en la Organización

En el artículo publicado por Gartner en Febrero de 2014 en el cual los autores (Peter Firstbrook, Neil MacDonald) hacen un análisis de la estrategia de seguridad aplicada mediante sistemas de protección de punto final y sistemas avanzados de detección y respuesta, plantean la Arquitectura de Seguridad Adaptativa y sus cuatro fases para fortalecer los esquemas de seguridad de las organizaciones frente a las amenazas modernas.

A continuación se presenta los puntos relevantes y las recomendaciones finales de los autores. Un mayor nivel de detalle puede ser consultado en *http://www.gartner.com/technology/reprints.do?id=1-1WTUFJJ&ct=140707&st=sb*.

Los fracasos de las organizaciones en detener los ataques dirigidos exigen repensar la estrategia de seguridad y equilibrar las inversiones en las cuatro fases de la arquitectura de seguridad adaptativa ASA (prevenir, detectar, responder y predecir) y adoptar una cultura de respuesta continúa. Las organizaciones deben asumir que están en peligro, y por tanto, invertir en capacidad para monitorizar

continuamente patrones y comportamientos indicativos de ataques, para esta labor están surgiendo herramientas que simplifican la tarea.

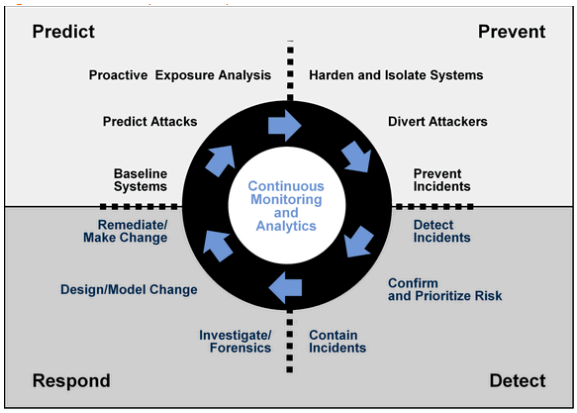
Todas las organizaciones ya están infectadas con malware, a pesar de lo que sus soluciones End Point Protection están reportando. Ante esto los proveedores de seguridad líderes tratan con la respuesta a incidentes como una actitud continua por lo cual actúan como bomberos esperando una alerta antes de iniciar la acción. Por otra parte otras organizaciones de seguridad más avanzadas actúan como detectives, ellos están investigando continuamente para descubrir eventos sospechosos que los llevaran al malware oculto. Estos proveedores están llenado el vacío dejado por las soluciones EPP, proveedores como Mandiant, Cisco Sourcefire, Negro de Humo, Promisec, RSA, Guidance Software y CounterTack proporcionan herramientas de detección y respuestas de amenazas de punto final.

Con la posibilidad de que la organización más allá de los controles establecidos se encuentre infectada, es necesario pensar en el cambio de estrategia de una actitud reactiva (respuesta a incidentes) a un proceso de detección y respuesta continua, invirtiendo en herramientas ETDR (End Point ThreatDetection) y procesos que puedan detectar las infecciones de malware que han evadido soluciones de bloqueo y prevención tradicionales así como fortalecer los controles establecidos como la gestión de la configuración y las herramientas automatizadas que la facilitan.

Actualmente muchos de los proveedores de EPP (End Point Protection) ubicados en el cuadrante mágico de Gartner se encuentran en un bucle sin generar firmas de amenazas conocidas. Con el tiempo han realizado ajustes a la estrategia defensiva, como firmas heurísticas y detección de comportamiento para familias de malware. Sin embargo la relativa facilidad con la que los atacantes pueden eludir estas técnicas preventivas cada vez es más evidente, sin que nada se haya intensificado para remplazarlos.

En el diseño de una arquitectura de seguridad adaptable de protección (ASA) contra los ataques avanzados, Gartner describe cuatro fases y 12 capacidades claves necesarias para que una empresa logre una estrategia de protección más integral. *Las cuatro etapas de la arquitectura ASA son Prevenir, Detectar, Responder, Predecir. Ver Figura 16.

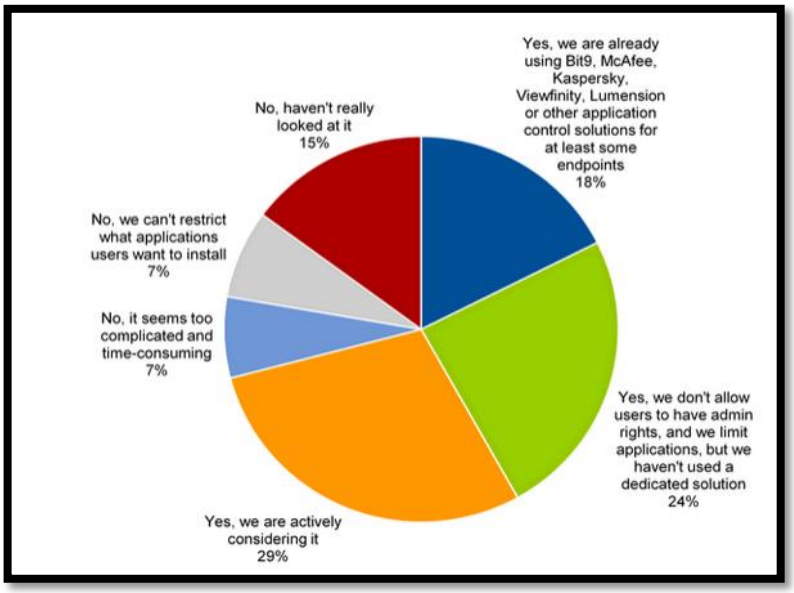
Figura 15. Ciclo de la Arquitectura de Seguridad Adaptable



Fuente: Gartner (Febrero 2014)

- **Prevenir:** Describe el conjunto de políticas, productos y procesos que se ponen en su lugar para evitar un ataque exitoso. El objetivo fundamental de esta etapa es el de reducir la superficie de ataque y prevenir ataques antes de que puedan afectar la empresa.
- **Detectar:** Capacidades diseñadas para encontrar ataques que han evadido la capa de prevención, su objetivo fundamental es reducir el tiempo de permanencia de las amenazas y por tanto reducir el potencial daño que pueden causar.
- **Responder:** Son competencias para remediar los problemas descubiertos por las actividades investigativas, proporcionar un análisis forense y recomendar nuevas medidas preventivas para evitar fracasos repetidos.
- **Predecir:** Permite a la organización aprender de los acontecimientos y de las fuentes externas para anticiparse proactivamente a nuevos tipos de ataques. Esto se usa como una entrada en las actividades preventivas y de detección.

Figura 17. Uso de herramientas EPP en las organizaciones



Fuente: Gartner Endpoint protection customer reference survey, 2013

De acuerdo con el análisis realizado por Gartner, la mayoría de las empresas buscan prevenir el 100% del malware con una sobrecarga administrativa mínima, y es por ello que los fabricantes de EPP se centran principalmente en las fases de prevenir. No obstante ha sido imposible proporcionar prevención perfecta, toda vez que los ataques exitosos tienen tiempos de espera muy largos, estos tiempos de espera largos ilustran que las organizaciones de TI carecen de la capacidad para detectar problemas y señales de alerta temprana que el malware ha dejado mediante controles que ha sobrepasado.

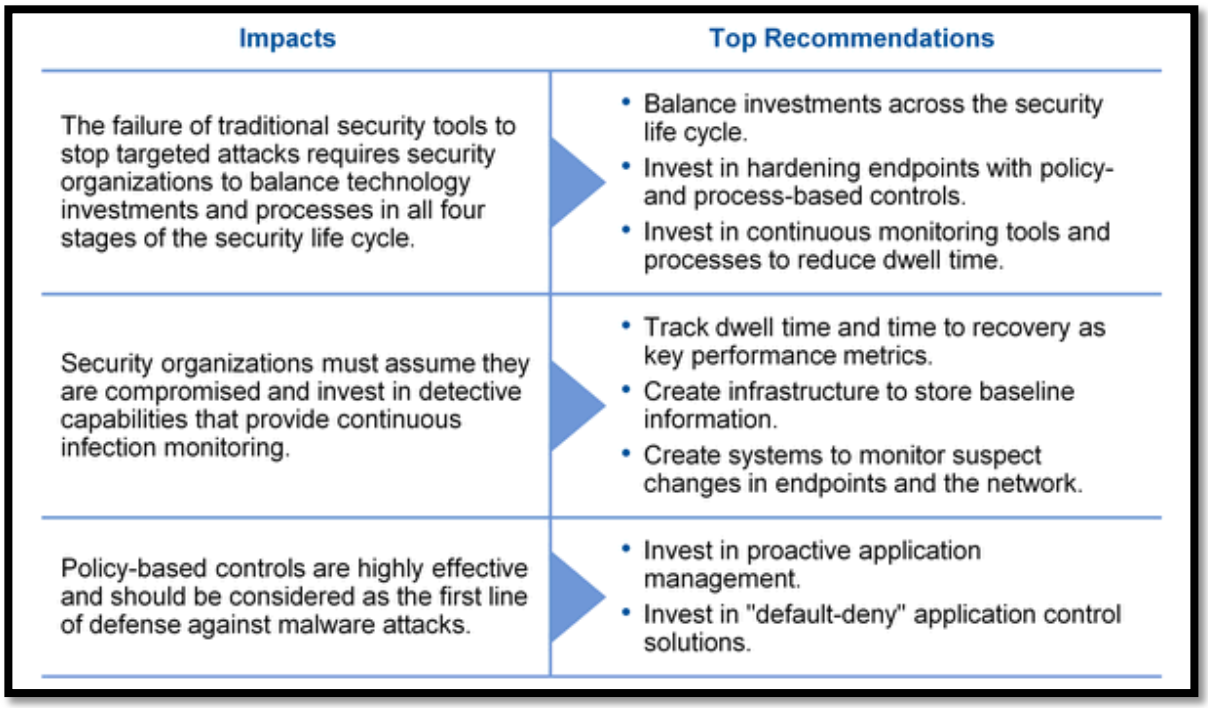
De acuerdo a la figura 17, la gestión proactiva es una tarea de enormes proporciones para organizaciones grandes, principalmente porque las herramientas para identificar y priorizar las actividades para reducir la superficie de ataque requieren de ajustes permanentes en su configuración. Sin embargo estudios han demostrado que las políticas de configuración correcta pueden reducir los incidentes en un 85%, así como el control de despliegue de aplicaciones es otro enfoque de seguridad de gran alcance, que a menudo es ignorado por las soluciones EPP a pesar que el interés del cliente en estas capacidades es bastante alto.

Gartner Group recomienda:

- Utilizar la arquitectura ASA para evaluar proveedores y equilibrar las inversiones en seguridad.

- No sobre-invertir en la prevención por sí sola, a expensas de endurecimiento y capacidades de detección.

Figura 16. Recomendaciones de Gartner Group para fortalecer la seguridad



Impacts	Top Recommendations
The failure of traditional security tools to stop targeted attacks requires security organizations to balance technology investments and processes in all four stages of the security life cycle.	• Balance investments across the security life cycle. • Invest in hardening endpoints with policy- and process-based controls. • Invest in continuous monitoring tools and processes to reduce dwell time.
Security organizations must assume they are compromised and invest in detective capabilities that provide continuous infection monitoring.	• Track dwell time and time to recovery as key performance metrics. • Create infrastructure to store baseline information. • Create systems to monitor suspect changes in endpoints and the network.
Policy-based controls are highly effective and should be considered as the first line of defense against malware attacks.	• Invest in proactive application management. • Invest in "default-deny" application control solutions.

Fuente: Gartner (February 2014)

- Favorecer proveedores EPP que entienden la necesidad de un ASA, así como los que proporcionan más capacidades coordinadas.

- Invertir en herramientas ETDR, capacidades y procesos que pueden detectar las infecciones de malware que han evadido soluciones de prevención tradicionales.

- Endurecer los controles preventivos de punto final, ampliar los procesos de gestión de parches para incluir navegadores alternativos y pluggins populares.

- Invertir en herramienta de gestión de la configuración y herramientas de control de aplicaciones para reducir los gastos generales de gestión del mantenimiento de los puntos finales.

- El control de aplicaciones, en particular, se debe considerar como una solución práctica para servidores, sistemas que no pueden ser parcheados y sistemas embebidos.

6.8.6 Re-imaginando la seguridad. La seguridad convencional detecta las amenazas demasiado tarde y les resuelve con demasiada lentitud. Los equipos de seguridad tienen una visión incompleta y fragmentada de lo que está pasando en su red. Es pasiva y ciego a tendencias de amenazas más amplias y reacciona con demasiada lentitud para nueva amenazas y las condiciones cambiantes.

Los ataques avanzados de hoy en día exigen un enfoque avanzado. Las organizaciones necesitan un marco flexible, profundamente integrado que ofrezca una visión de largo alcance de las amenazas y que evolucione a medida como las condiciones lo hacen.

Mediante la adopción de una estrategia de seguridad adaptativa, las organizaciones pueden obtener, protección integrada de extremo a extremo de la red de entrada hasta el punto final. Consiguen una vista del panorama general de la actividad de su atacante a través de su red completa. Pueden integrar inteligencia para no sólo responder a las amenazas, sino también para anticiparlos de forma oportuna.

6.8.7 Hay que Girar Hacia la Seguridad Adaptativa. La seguridad adaptativa consiste en algo más que solo tecnologías, habilidades o procesos. Mientras que el concepto incluye todos estos, se trata de una nueva forma de pensar fundamentada en los nuevos ataques cibernéticos. En lugar de tratar de evitar los ataques, las organizaciones que implementan una defensa adaptativa tienen un enfoque orientado en detectar rápidamente los ataques y luego responder para evitar los peores resultados. En el modelo de adaptación, los equipos de seguridad tienen las herramientas de inteligencia, y experiencia para detectar, prevenir, analizar, y resolver a medida que los ataques avanzados cambian sus estrategias.

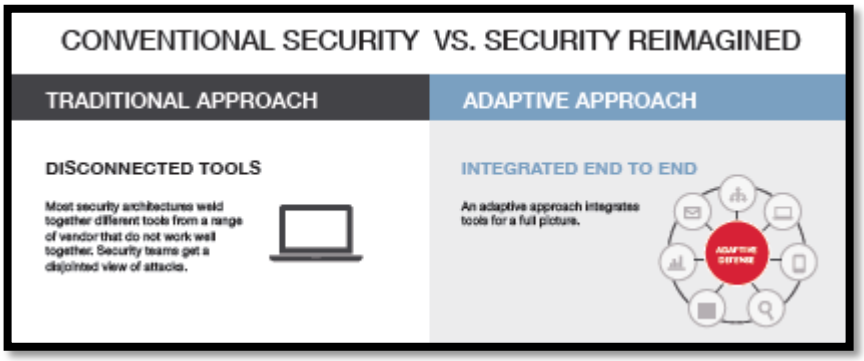
El objetivo es reducir principalmente dos métricas:

- Tiempo para detectar
- Tiempo para resolver

Se Necesita una Defensa Integrada End to End

Mientras que en el modelo convencional existe una mezcla de herramientas de diferentes proveedores, cada uno centrado en un objetivo específico, que no facilita a los analistas obtener un nivel de correlación para detectar un ataque avanzado, inclusive si cada herramienta funciona correctamente y se genera una visión fragmentada de la seguridad, la estrategia de seguridad adaptativa, no solo ve ataques de múltiples vectores de amenazas y de flujos sino también conecta los puntos para dar a los equipos de seguridad una imagen completa de los eventos, logrando que los equipos de seguridad no solo vean indicios sino que consiguen una imagen completa para que detallar el ciclo de vida del ataque a cada paso, desde la infección del malware hasta el reconocimiento de los datos fugados.

Figura 19. Seguridad Convencional Vs Seguridad Adaptativa



Fuente: FireEye, security reimagened – White paper 2014.

En el modelo adaptativo los analistas pueden ver como el tráfico en el perímetro se refiere a los cambios del sistema operativo de un PC conectado a la red y puede reconstruir semanas de tráfico de red para rastrear la fuente del ataque.

Un modelo de adaptación no sólo arroja datos en bruto. En su lugar, ayuda a darles sentido a dichos datos. Por el análisis de tráfico de red inusual, archivos sospechosos y la inteligencia de amenazas, el sistema de seguridad ideal puede correlacionar eventos aparentemente no relacionados para detectar ataques que de otro modo podrían perderse en el ruido.

Con una estrategia de adaptación, los usuarios no tienen la acostumbrada avalancha de falsas alarmas, advertencias crípticas e informes. En su lugar, se disponen de alertas que dan información precisa, de alta prioridad y que puede utilizar para contener y resolver rápidamente las amenazas.

A diferencia de las arquitecturas de seguridad tradicionales, una estrategia adaptativa se posiciona para responder instantáneamente a las amenazas conocidas y desconocidas. En este sentido, agilidad implica detectar rápidamente y determinar que contienen estas amenazas. El enfoque de adaptación se centra en detener los ataques antes de que lleguen evitando resultados perjudiciales sin recurrir a su detención en el perímetro y adaptándose rápidamente a las amenazas cambiantes.

7. CONCLUSIONES

En el anteproyecto se formuló la siguiente pregunta problema:

¿Qué elementos se deben incorporar o modificar en una arquitectura de seguridad para prevenir, detectar, contrarrestar y en general fortalecer la protección contra las APT en la ANH que ha basado su estrategia de protección en el modelo de defensa en profundidad?

Y se formularon las siguientes hipótesis:

H1: El modelo en Defensa en profundidad de la ANH se fortalecerá mediante la aplicación de estrategias o mecanismos de control para detectar la presencia, prevenir o reaccionar a ataques tipo APT.

H0: En la ANH no es posible fortalecer el modelo de defensa en profundidad mediante la aplicación de estrategias o mecanismos de control para prevenir y reaccionar a ataques tipo APT.

La primera conclusión del grupo de estudio es que se valida la hipótesis H1, esto es, el modelo de defensa en profundidad no riñe con los nuevos modelos de protección sugeridos (seguridad adaptativa) sino que le alimenta, esto es, no se puede implementar un modelo de seguridad adaptativa sin contar con mecanismos básicos de defensa perimetral, si se llegara a ello se estaría promoviendo un enfoque reactivo sin información para analizar y reduciendo los niveles de protección alcanzados.

En cuanto a la pregunta problema, se formulan las siguientes recomendaciones:

- Es necesario trabajar fuertemente en la concienciación y creación de cultura en seguridad de la información. Este reto ha sido un obstáculo grande en las organizaciones y se incrementa para lograr la compresión de las amenazas avanzadas persistentes.

- El modelo de Defensa en Profundidad es insuficiente frente a las APT pero no contar con él significa mayores niveles de exposición. En nuestra opinión la adquisición o implementación de soluciones de APT´s deben verse como la capa de detección y respuesta del modelo de Defensa en Profundidad.

- Dar el giro hacia la seguridad adaptativa significa más que adquirir soluciones APT´s. Se requiere fortalecer el modelo de Defensa en Profundidad y contar con equipo de respuesta a incidentes mucho mejor estructurados, entrenados y capacitados.

Se considera prudente realizar las siguientes recomendaciones en aras de fortalecer el contenido temático de la especialización de Seguridad Informática:

- Profundizar en la formación y desarrollo de competencias en gestión de seguridad de la información. Como se pudo observar a lo largo del proyecto, la seguridad de la información no sólo comprende soluciones de tecnología sino que requiere de una estrategia para implementar, impulsar y mantener los programas de seguridad.

- Incluir conceptos para diseñar, implementar y mantener equipos de respuesta a incidentes con las competencias requeridas en la actualidad y las que nos imponen las nuevas amenazas.

BIBLIOGRAFÍA

CISCO. SAFE Reference Guide. Cisco Validated Design. July 8, 2010.

CISCO. DNS Best Practices, Network Protections, and Attack Identification.

INFORMATION SYSTEMS SECURITY ARCHITECTURE PROFESSIONAL. Official (ISC)2 Guide To the ISSAP CBK. CRC Press. 2010.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO - IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements.2013-

ISACA. Business Model For Information Security.

ISACA. E-Commerce Security: Securing The Network Perimeter, 2004.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Border Gateway Protocol Security. Special Publication 800-54. July 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Electronic authentication guideline NIST SP 800-63-2. August 2013.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to Intrusion Detection and Prevention Systems (IDPS). Special Publication 800-94. February 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to IPsec VPNs. Special Publication 800-77 .December 2005.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to SSL VPNs. Special Publication 800-113. July 2008.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guidelines on Firewalls and Firewall Policy. Special Publication 800-41. September 2009.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cibersecurity, Version 1.0, February. 2014.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST 800 – 14 Generally Accepted Principles and Practices for Securing Information Technology Systems.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST 800 – 30 Risk Management Guide For Information Technology Systems.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Special publication 800-39, Managing information security risk, organization, misión and information systems, EEUU. 2011.

MERCHÁN PATARROYO RAMIRO. Seminario Seguridad de la Información, Universidad de la Sábana.2014.

STALLINGS WILLIAM Y BROWN LAWRIE. Computer Security, Principles and Practice, 3 Edition. Pearson Editorial, 2014.

www.anh.gov.co.

www.checkpoint.com/.

www.fireeye.com/.

http://www.gartner.com/technology/

www8.hp.com/us/en/software-solutions/network-security/

www.iboss.com/.

www.sans.org.

www.verint.com.

www.wikipedia.org/wiki/prueba_de_concepto

ANEXO A. Divulgación

TRABAJO DE GRADO

FORTALECIMIENTO DEL ESQUEMA DE DEFENSA EN PROFUNDIDAD EN LA ANH PARA INCREMENTAR EL NIVEL DE PROTECCIÓN FRENTE A LAS AMENAZAS PERSISTENTES AVANZADAS.

DIEGO CARRILLO RICO

RAMIRO MERCHAN PATARROYO

ESPECIALIZACION EN SEGURIDAD INFORMATICA

UNIVERSIDAD PILOTO DE COLOMBIA

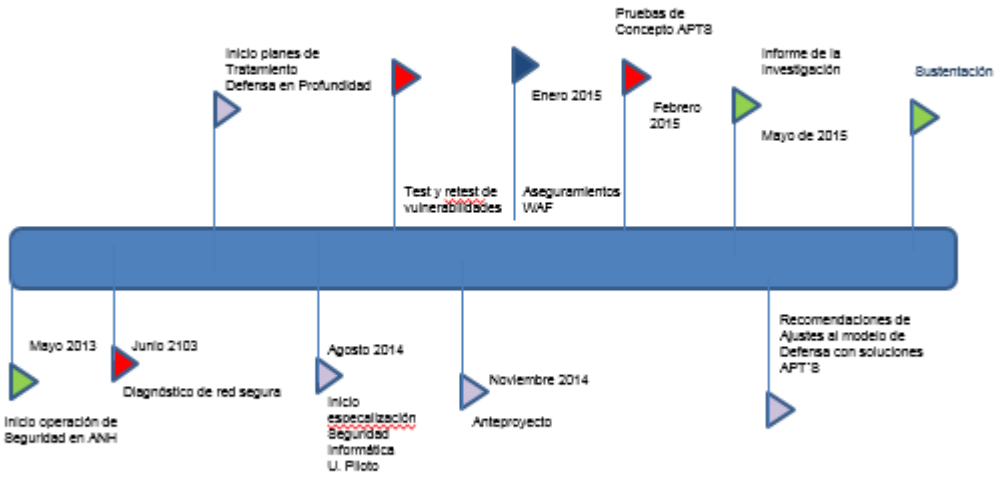
Bogotá, septiembre 1 de 2015

FORTALECIMIENTO DEL MODELO DE DEFENSA EN PROFUNDIDAD PARA CONTRARRESTAR LAS APT´S EN LA ANH

AGENDA

- Pregunta problema
- Presentación de la ANH
- Conceptos de Defensa en Profundidad
- Conceptos de APT´s
- Implementación de Seguridad
- Identificación de APT´s presentes en la infraestructura
- Conclusión

LINEA DE TIEMPO DE LA INVESTIGACION



PREGUNTA PROBLEMA

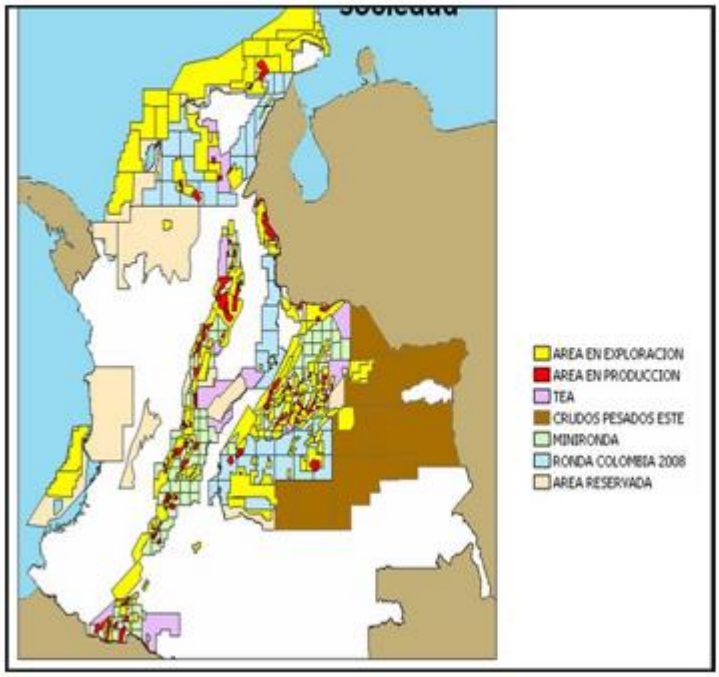
¿Qué elementos se deben incorporar o modificar en una arquitectura de seguridad para prevenir, detectar, contrarrestar y en general fortalecer la protección contra las APT en la ANH que ha basado su estrategia de protección en el modelo de defensa en profundidad?

HIPOTESIS FORMULADAS

H1: El modelo en Defensa en profundidad de la ANH se fortalecerá mediante la aplicación de estrategias o mecanismos de control para detectar la presencia, prevenir o reaccionar a ataques tipo APT.

H0: En la ANH no es posible fortalecer el modelo de defensa en profundidad mediante la aplicación de estrategias o mecanismos de control para prevenir y reaccionar a ataques tipo APT.

PRESENTACION DE LA ANH – AGENCIA NACIONAL DE HIDROCARBUROS

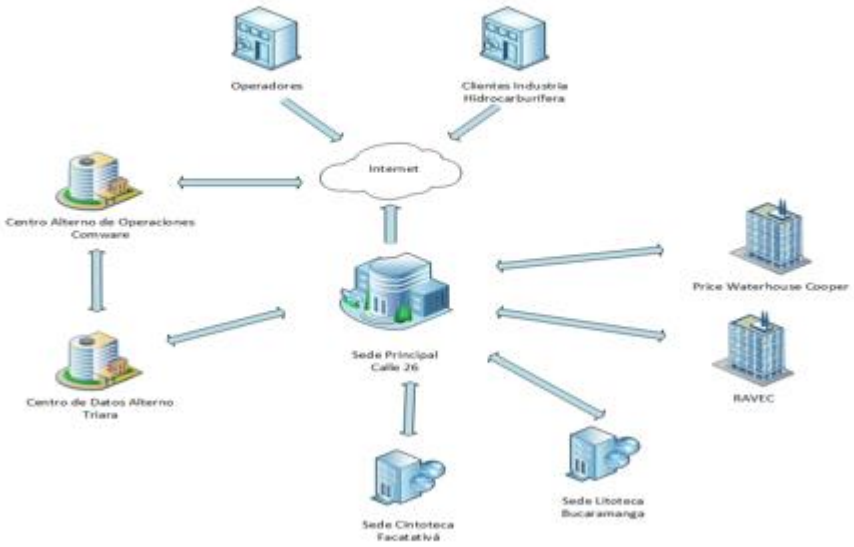


En el 2003 se consolidó la reestructuración del sector hidrocarburífero colombiano con la creación de la Agencia Nacional de Hidrocarburos como respuesta a la situación crítica que atravesaba Colombia debido a la disminución de las reservas de petróleo, lo cual eventualmente, llevaría al país a convertirse en importador de crudo.

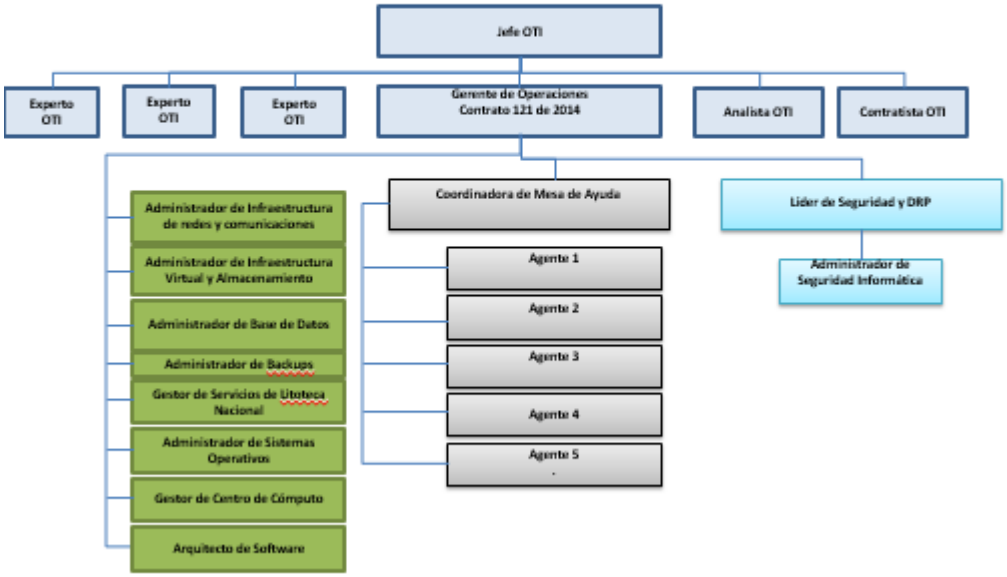
De esta forma, la Agencia Nacional de Hidrocarburos adquirió de Ecopetrol su labor de administrador y regulador del recurso hidrocarburífero de la nación, y comenzó la transformación de Colombia en un país nuevamente prospectivo y atractivo para los inversionistas nacionales y extranjeros.

Nuevo modelo de contratación
- Exploración
- Evaluación
- Explotación

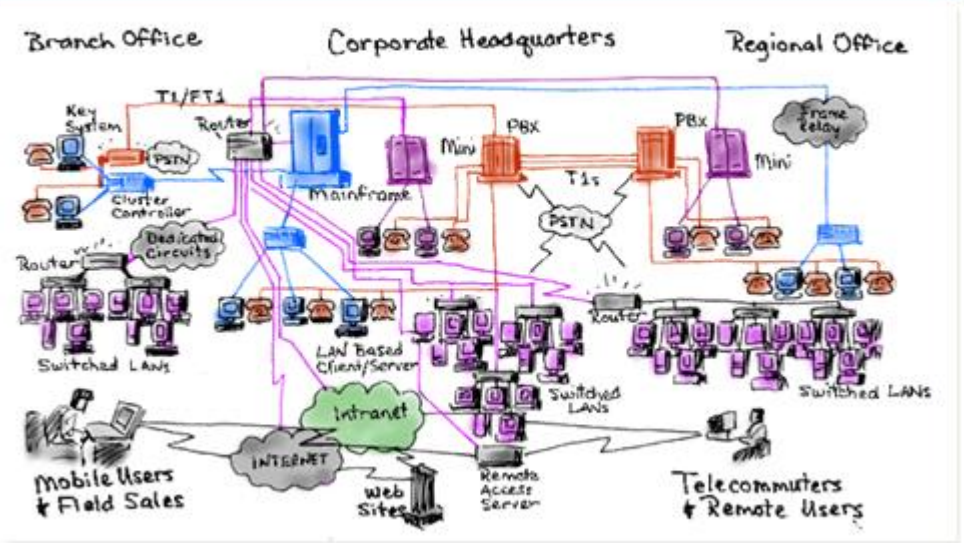
DIAGRAMA CONCEPTUAL DE TIC´S ANALIZADO



EQUIPO DE TRABAJO DE TECNOLOGIA



El Crecimiento Heterogéneo de las Redes de Computadoras

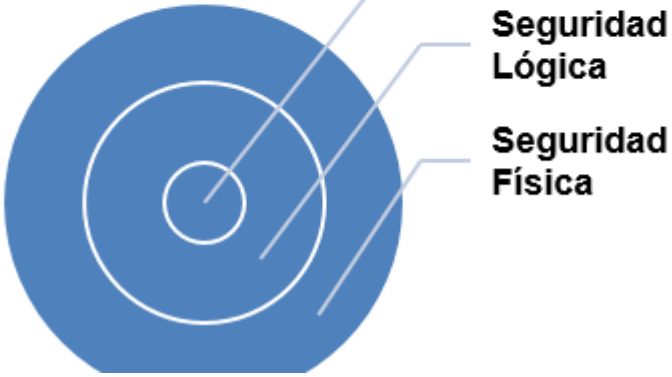


Defensa en Profundidad

•Si todo lo que se encuentra entre su información mas sensible y un atacante es una sola capa de seguridad, el trabajo del atacante se hace sencillo.

•Ninguna medida de seguridad; y en un concepto mas amplio, ninguna capa de seguridad, es infalible contra los ataques. Al agregar capas independientes a la arquitectura de seguridad se aumenta el tiempo que puede tomar el atacar un sitio, lo que permitiría en ultimas detectar las intrusiones y los ataques justo cuando estos ocurren.

•La filosofía "Defense in Depth" establece que: "los sistemas de seguridad de un sistema deben ser entendidos y contenidos dentro de capas, cada una independiente de la anterior de forma funcional y conceptual".



Defensa en Profundidad

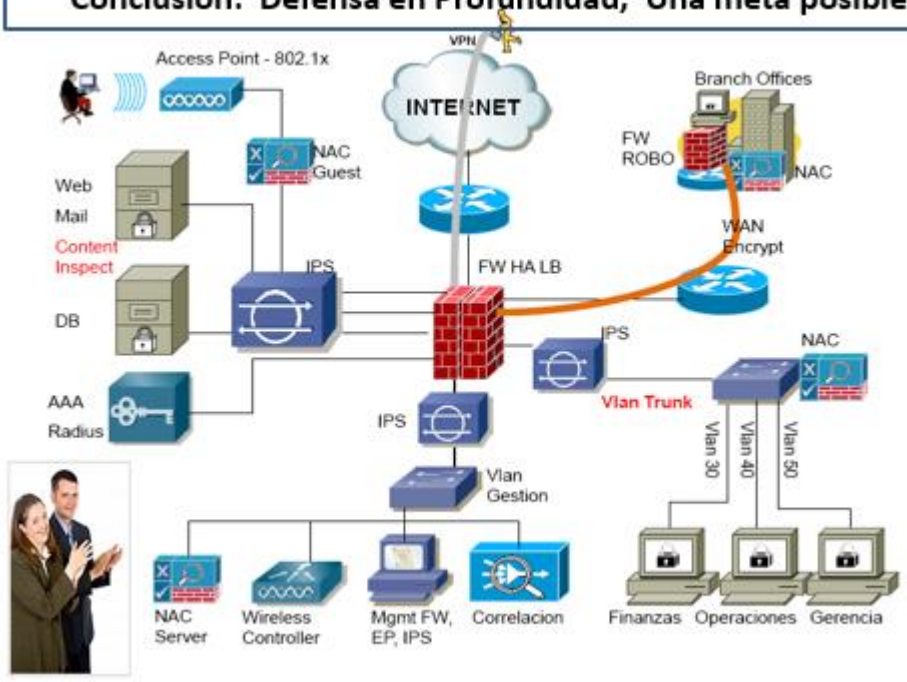
CONCEPTOS DE DISEÑO

- EVALUACIÓN DE RIESGOS
- ESTRATEGIAS Y ESTÁNDARES
- ZONAS SEGURAS
- ENDURECIMIENTO DE SISTEMAS
  - Endurecimiento del Sistema Operacional
  - Eliminar servicios no requeridos
  - Actualización periódica de parches (sistemas operativos y aplicaciones)
  - Desactivar protocolos no encriptados
  - Protección contra virus
  - Renombrar cuentas de administrador
  - Cambiar passwords por defecto
  - Desactivar cuentas de invitado
  - No permitir anonimus FTP
  - Incrementar tamaño de archivos de log
  - Permisos sobre directorios, archivos y otros objetos
  - Desplegar mensajes de alerta
  - Implementar el concepto de menor privilegio
  - Separación de funciones

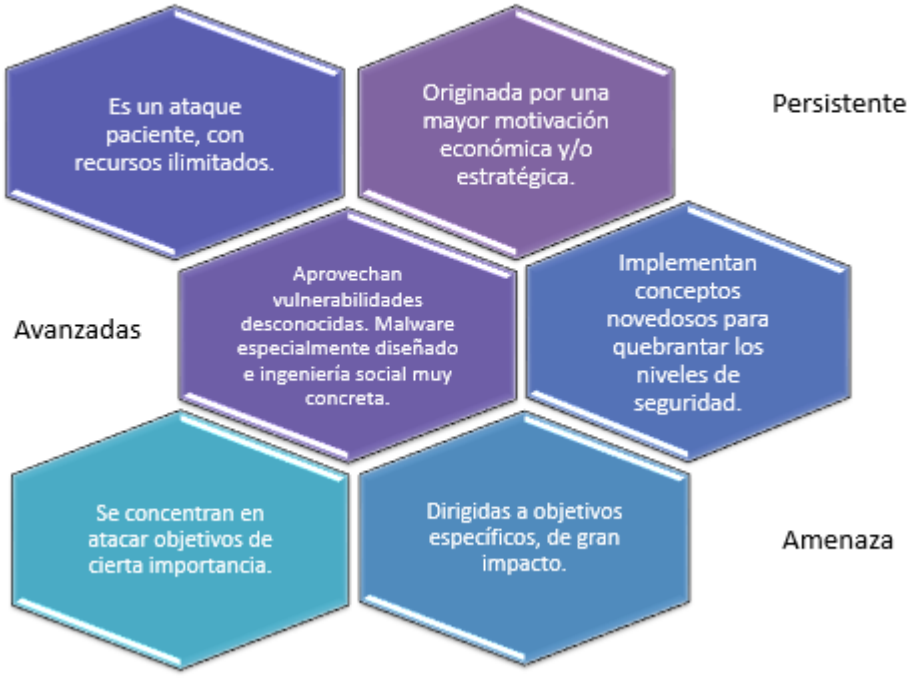
COMPONENTES

- ENRUTADORES
- SWITCHES
- FIREWALLS
- ACCESO REMOTO – VPN
- ACCESO REMOTO – DIAL UP
- REDES INALAMBRICAS
- DETECCIÓN DE INTRUSIONES
- EVALUACION DE LA SEGURIDAD DE LA RED
  - Análisis de vulnerabilidades

Conclusión: Defensa en Profundidad, Una meta posible



Amenazas Persistes Avanzadas (APT) Características



Amenazas Persistes Avanzadas (APT)
Proceso de ataque

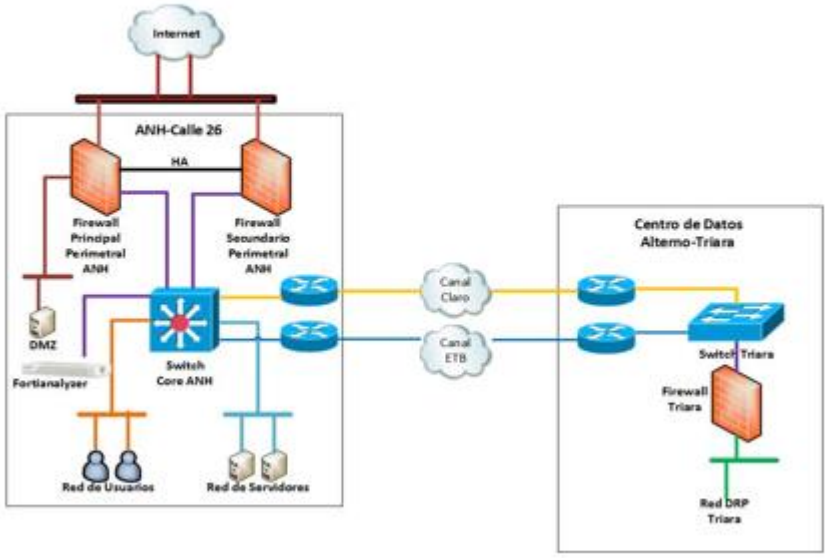
Estudio de la victima → Infección → Propagación

METODOS DE INFECCIÓN Y PROPAGACIÓN

- Ingeniería Social
- BYOD
- Vulnerabilidades persistentes en la infraestructura
- Phishing dirigido
- Debilidades en las defensas perimetrales
- Ataques señuelo

EVALUACION DE RED SEGURA

- Diseño Inicial



Evaluación de Red Segura – Defensa en Profundidad

Probabilidad de riesgo	Severidad del Riesgo				
	Catastrófico A	Crítico B	Moderado C	Menor D	Despreciable E
5 – Frecuente	5A	5B	5C	5D	5E
4 – Probable	4A	4B	4C	4D	4E
3 – Ocasional	3A	3B	3C	3D	3E
2 – Raramente	2A	2B	2C	2D	2E
1 – Improbable	1A	1B	1C	1D	1E

IPS	Se recomienda que se encuentre lógicamente ubicado entre el firewall de frontera y el Core Administración de alertas y monitoreo Dispositivo en redundancia Use una interfaz exclusiva para administración	-En la actualidad ANH posee la funcionalidad de IPS perimetral dentro del sistema UTM perimetral. - No mantiene una interfaz exclusiva de administración.	6B
WAF	Configurar WAF para aplicaciones criticas (como aplicaciones transaccionales)	No se tiene evidencia que existan WAF.	6B
Monitoreo, análisis y correlación	Se recomienda tener un dispositivo centralizado para administrar los eventos y tráfico de los dispositivos	Se cuenta con el dispositivo pero con nivel de configuración básico	6B

	A	B	C	D	E
5		26,34,35,41,43,50,51,53,54	14,21,25,61		
4	7	32,33,42	5,8,15,16,17,19,58		
3		10,11,22	18,20,38,39,40,46	4,44	
2		1,6	2,9,13		
1		23,24,48,49,52	12,30,45	36,37,47	

Evaluación de Red Segura – Resumen General

DATOS
- En la actualidad ANH no cuenta con seguridad dedicada para proteger las Bases de datos de ataques o accesos no autorizados

APLICACIONES
- La conexión existente entre las aplicaciones, datos y usuarios se maneja a un mismo nivel. Generando uni dificultad de protecciones multinivel.
- Se maneja AntiSpam para la protección de correo entrante.

HOST
- Se cuenta con herramientas con DLP de McAfee
- Es necesario reforzar el uso de EndPoint para protección interna y dispositivos móviles

REDES
- El único dispositivo de protección a las redes es el UTM perimetral

PERÍMETRO
- ANH cuenta con un dispositivos de seguridad perimetral UTM, el cual brinda la primera fase de protección para toda la red.

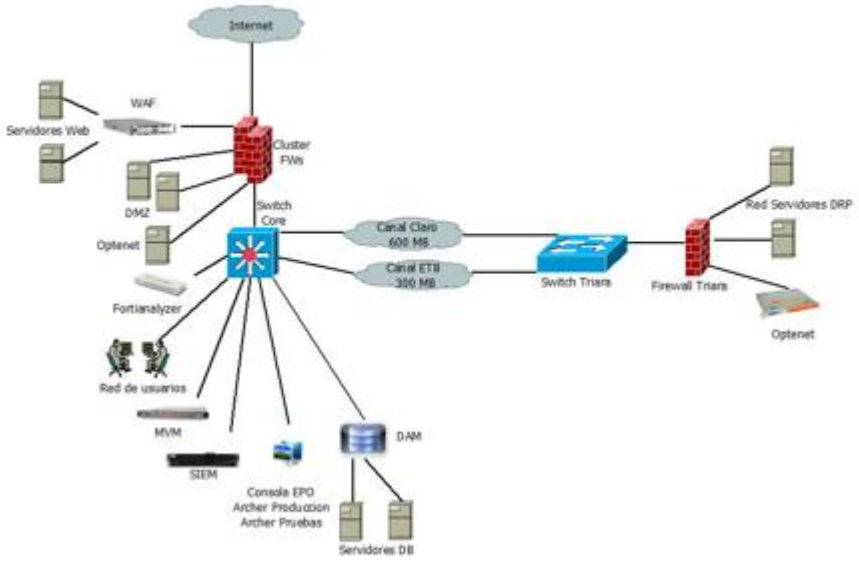
POLÍTICAS y MONITOREO
- La definición de políticas de seguridad está incipiente, lo que genera faltas en seguridad por desconocimiento.
- ANH cuenta con un grupo de herramientas de apoyo a la seguridad, sin embargo estas están en un estado básico de configuraciones.

Avance en Planes de Tratamiento

FASE	OBJETIVO	ACTIVIDADES DESARROLLADAS
Planear	Alcance del SGSI	Estructura de las políticas de seguridad
	Política	Estructura de las políticas de seguridad
	Inventario de activos	Inventario de información de usuarios, línea base del EPIS
	Análisis de riesgos	Matriz de riesgos de gestión de tic, matriz de riesgos de disponibilidad
	Controles a implementar	Recomendaciones de red segura, políticas de seguridad
	Planes de tratamiento	Recomendaciones de red segura, recomendaciones de gestión de vulnerabilidades, Seguridad informática
	Declaración de aplicabilidad	Estructura de las políticas de seguridad
Hacer	Ejecución de planes de tratamiento	Implementación de recomendaciones de red segura, aseguramientos
	Implementación de políticas	Fortalecimiento de seguridad informática, DRP
	Entrenamiento	Campañas de concientización
	Operación	Fortalecimiento del grupo TIC de la OTI. Informes mensuales de operación, Pruebas DRP
	Registro de incidentes	Procedimiento de gestión de incidentes

EVALUACIÓN DE RED SEGURA

- Diseño actual



Arquitectura de seguridad adaptativa en cuatro fases

Amenazas Persistes Avanzadas (APT)
Herramientas de protección

	Detectar	Prevenir	Analizar	Resolver
Iboss	•			
Tipping Point	•	•	•	•
FireEye	•	•	•	•
Verint TPS	•	•	•	•

FireEye

Web Security: Inspecciona y protege el trafico web entrante o saliente, ejecutando ejecución virtual, dinámica y en tiempo real de amenazas de amenazas Web, útil para atacar amenazas tipo zero-day.

Email security: Inspecciona todos los documentos adjuntos y URLs incluidas en correos. Aísla y analiza los exploits de programas malintencionados y los ataques usualmente usados en phishing.

Malware análisis: Mediante un entorno seguro, los analistas pueden hacer ejecutar y revisar detalladamente programas malintencionados.

Malware protection cloud: Realiza intercambio global en tiempo real de información sobre amenazas que ayudan a anticipar la aparición de amenazas de tipo zeroday.

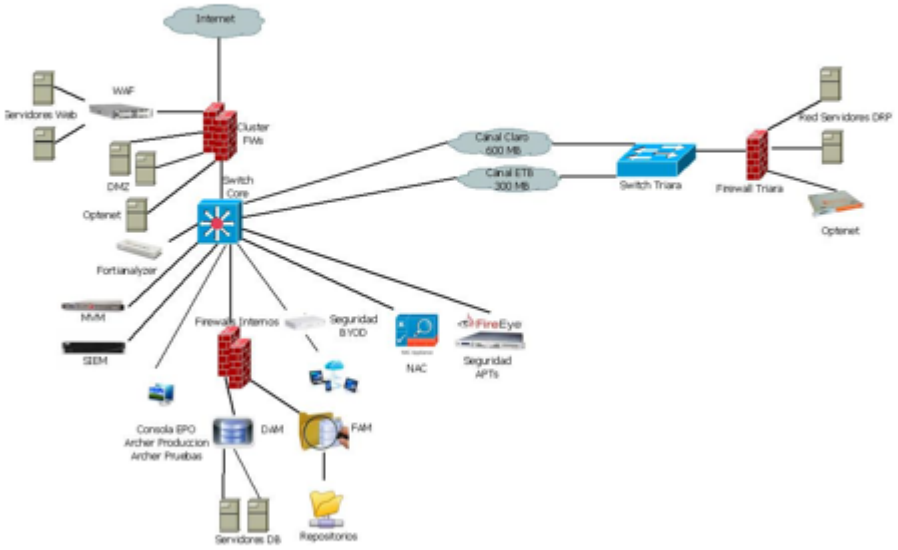
Central Managment system: Incluye una consola de administración centralizada, que permite consolidar información y los datos compartidos por las plataformas FireEye.

EVALUACION DE APT´S – POC FIREYE

Malware encontrado	Descripción	Host Afectados
Bot Conficker	<<<Es un gusano informático que ataca sistemas operativos Windows. El gusano tiende a propagarse por medio de desbordamiento de buffer de algunos servicios Windows.	1
Malware Zeroday Callback	Está clasificado como malware, el cual tiene como objetivo infectar una máquina para así realizar función de Botnet. El objetivo de este tipo de malware, tiende a ser el robo de información o uso ilegal para no ser detectados en la red, y así generar ataques que permitan suplantar el origen	2
InfoStealer Generic	Infostealer es una amenaza muy peligrosa. Realiza un seguimiento de las pulsaciones de teclado. Puede disminuir el rendimiento del sistema y lleva a la parada brusca del ordenador. Puede bloquear el equipo y en el peor de los casos exige dinero para recuperar el problema. Cambia la página de inicio y redirige las búsquedas completas de los sitios Web maliciosos. Tiene capacidad para entrar automáticamente en el sistema del usuario sin el consentimiento del mismo.	1
Malware Binary	Es una clasificación para ciertos tipos de malware, que son adquiridos por descargas a través de internet. El usuario se infecta a partir de la ejecución de programas que no son lo que aparentan. Al igual que las amenazas anteriores, son usados para alterar registros de Windows, robo de información sensible	2
Total Malware Encontrados		12

DEFENSA EN PROFUNDIDAD – ARQUITECTURA DE RED RECOMENDADA

- Diseño Ideal



CONCLUSIONES

La conclusión del grupo de estudio es que se valida la hipótesis H1, esto es, el modelo de defensa en profundidad no riñe con los nuevos modelos de protección sugeridos (seguridad adaptativa) sino que le alimenta, esto es, no se puede implementar un modelo de seguridad adaptativa sin contar con mecanismos básicos de defensa perimetral, si se llegara a ello se estaría promoviendo un enfoque reactivo sin información para analizar y reduciendo los niveles de protección alcanzados.

En cuanto a la pregunta problema, se formulan las siguientes recomendaciones:

1. Es necesario trabajar fuertemente en la concienciación y creación de cultura en seguridad de la información. Este reto ha sido un obstáculo grande en las organizaciones y se incrementa para lograr la compresión de las amenazas avanzadas persistentes.

2. El modelo de Defensa en Profundidad es insuficiente frente a las APT pero no contar con él significa mayores niveles de exposición. En nuestra opinión la adquisición o implementación de soluciones de APT´s deben verse como la capa de detección y respuesta del modelo de Defensa en Profundidad.

3. Dar el giro hacia la seguridad adaptativa significa más que adquirir soluciones APT´s. Se requiere fortalecer el modelo de Defensa en Profundidad y contar con equipo de respuesta a incidentes mucho mejor estructurados, entrenados y capacitados.

Fortalecimiento del Esquema de Defensa en Profundidad para incrementar el nivel de protección frente a las Amenazas Persistentes Avanzadas

Merchan, Ramiro. Carrillo, Diego.
Universidad Piloto de Colombia

Resumen—El presente documento realiza un análisis del modelo de defensa en profundidad de la organización frente a las APT para determinar si es suficiente, puede adaptarse o definitivamente no es suficiente para protegerla ante las amenazas persistentes avanzadas.

Índice de Términos—defensa en profundidad - amenazas persistentes avanzadas - arquitectura de red segura - diagnóstico de seguridad.

Abstract—This document analyzes the pattern of defense in depth against the APT organization to determine if sufficient, can adapt or definitely not enough to protect against advanced persistent threats.

Index Terms—Defense in depth - advanced persistent threats - secure network architecture - security diagnosis.

I. INTRODUCCIÓN

Este artículo presenta el análisis y las recomendaciones para fortalecer el modelo de defensa en profundidad en una organización gubernamental frente a las amenazas persistentes avanzadas.

En un proyecto que se desarrolló con el propósito de resolver la pregunta: ¿Qué elementos debe agregar o cambiar una arquitectura de seguridad para prevenir, detectar, disuadir y, en general fortalecer la protección contra las APT en las organizaciones que han basado su estrategia en materia de protección bajo el modelo de defensa en profundidad?

Se presentan los conceptos del esquema de defensa en profundidad y las amenazas persistentes avanzadas, incluyendo los análisis de red segura y vulnerabilidades técnicas de la organización, para generar recomendaciones orientadas al fortalecimiento de la arquitectura de red inicial.
También integra la implementación y los resultados de una prueba de concepto sobre una herramienta de protección de APT, las conclusiones sobre la eficacia del modelo de seguridad y recomendaciones para reducir aún más la probabilidad de éxito de este nuevo tipo de ataque desde el marco de la seguridad adaptativa.

II. CONCEPTOS TEÓRICOS

A. El modelo de defensa en profundidad

La filosofía Defensa en Profundidad establece que "los sistemas de seguridad de un sistema deben ser entendidos y contenidos dentro de capas, cada una independiente de la anterior de forma funcional y conceptual".

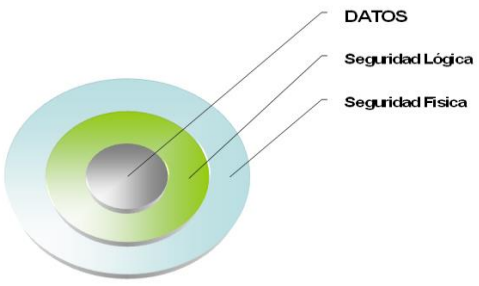


Fig 1. El modelo de defensa en profundidad. ISACA – E-Commerce Security.Securing The Network Perimeter, 2004

El modelo recomienda no olvidar los siguientes postulados:

- Si todo lo que se encuentra entre su información más sensitiva y un atacante es una sola capa de seguridad, el trabajo del atacante se hace sencillo.
- Ninguna medida de seguridad; y en un concepto más amplio, ninguna capa de seguridad, es infalible contra los ataques.
- Al agregar capas independientes a la arquitectura de seguridad se aumenta el tiempo que puede tomar el atacar un sitio, lo que permitiría en últimas detectar las intrusiones y los ataques justo cuando estos ocurren.

B. Amenazas Persistentes Avanzadas (APT)

El termino Amenazas Persistentes Avanzadas (APTs) se ha posicionado en la industria de la seguridad tanto de empresas de los sectores privado como Gubernamentales, para identificar los tipos de riesgos de ciberseguridad que por sus características pueden generar impactos mayores que las amenazas actuales.

Entre los principales rasgos de las APT se tienen:

- La capacidad de perdurar en el tiempo.
- La capacidad para aprovecharse de vulnerabilidades oficialmente desconocidas
- El estar dirigidas a objetivos específicos.

Aunque en definitiva las APT tratan de comprometer una red de computadores para conseguir información sensible, se ha posicionado como principal objetivo de las APT el espionaje empresarial, gubernamental y militar. Obteniendo y manipulando información contenida en los sistemas de la organización atacada, sin concentrase específicamente en atacar objetivos físicos.

III. EVALUACIÓN DEL MODELO DE DEFENSA EN PROFUNDIDAD

Si bien la valoración de la seguridad de la información comprende: evaluaciones de riesgos de T.I., pruebas de ingeniería social, evaluación de la seguridad física de los centros de cómputo, pruebas de vulnerabilidad, evaluación de red segura, entre otras, en el presente estudio se profundizo en dos actividades centrales para los objetivos propuestos:

- Evaluación de la seguridad de red bajo el modelo de defensa en profundidad.
- Análisis de vulnerabilidades técnicas.

A. Propuesta de evaluación de arquitectura de red segura.

La constante evolución del mundo de la seguridad lleva a las organizaciones a un continuo cambio. La rápida proliferación de bootnets, el incremento sofisticado de ataques de red, el amplio crecimiento de crímenes y espionaje basados en Internet, el robo de identidad y datos, y nuevas formas de ataques sobre los sistemas, son ejemplos de los diversos ataques a los que el mundo de la seguridad se está enfrentando. Como un factor clave de la actividad empresarial, las redes deben ser diseñadas e implementadas teniendo en mente la seguridad, para así asegurar la confidencialidad, integridad y disponibilidad de los datos y recursos que soportan las funciones claves del negocio. La evaluación de red se debe realizar con base en las buenas prácticas de acuerdo con estándares internacionales, como NIST y SANS y fabricantes como CISCO, Check Point, entre otros.

Lograr el nivel adecuado de seguridad, depende de la interrelación de todos los elementos, no solo dispositivos de seguridad como firewalls, IPS, Antivirus, sino de la unión de éstos con los dispositivos de Networking y Switching. Es por esto que el diagnóstico de seguridad adopta un enfoque en defensa en profundidad, donde múltiples capas de protección son estratégicamente configuradas.

En general, el diseño e implementación de una Arquitectura de red Segura debe estar basada en los principios de defensa en profundidad, modularidad y flexibilidad, disponibilidad y capacidad de recuperación, cumplimiento de regulaciones, e implementaciones auditables. La base de la Defensa en Profundidad se concentra en:

- Proteger: Aplicar controles y mecanismos preventivos.
- Detectar: Identificar y esperar ataque.
- Reaccionar: Responder ante ataques y recuperarse

El alcance de la evaluación de red segura se debe concentrar en:

- Protecciones de Elementos de red Generales.
- Frontera Internet.
- Frontera WAN.
- Monitoreo, Análisis y Correlación

B. Análisis de vulnerabilidades

Se recomienda a la organización implementar las siguientes prácticas para la gestión de vulnerabilidades:

- Grupos de Activos: Es necesario crear los grupos de activos considerando el valor que tiene para el negocio este activo en particular, es decir los grupos deben crearse de acuerdo a la criticidad de cada uno de sus miembros: Sistemas operativos, bases de datos, servicios de red.
- Planeación de remediación: Concertar con los administradores de las plataformas los tiempos de remediación de las vulnerabilidades críticas, medias y bajas que se identifiquen.
- Remediación: Realizar la remediación de las vulnerabilidades iniciando primero por las críticas y después pasar a las medias y bajas.
- Escaneos periódicos: Realizar escaneos iniciando por aquellos equipos que se consideren críticos para la organización. Algunos de los escaneos a realizar son:
  - SANS/FBI Top 20 Scan
  - Single VulnerabilityScan
  - Full Vulnerability Scan
  - WWW Application Assessment Scan
- Automatización: Programar la ejecución automática, programada y periódica de escaneos de acuerdo con el levantamiento de información realizado para grupos de activos y cantidad de vulnerabilidades críticas encontradas. Tentativamente se propone una periodicidad inicial de 6 meses.
- Notificación: Activar las notificaciones vía email con el fin que los administradores de plataforma tengan una visualización de las vulnerabilidades a remediar sobre los servidores/equipos que gestionan.
- Aplicaciones WEB: Evaluar de manera periódica las aplicaciones WEB.

IV. DETECCION DE AMENAZAS AVANZADAS PERSISTENTES

Aunque dentro de la organización se tenía la percepción de seguridad debido al fortalecimiento de su modelo de defensa en profundidad las características de la organización al estar ubicada en el sector Gobierno en actividad dentro de uno de los sectores críticos del país implica un riesgo considerable que hace necesario realizar una evaluación de la vulnerabilidad frente a las Amenazas Persistentes Avanzadas y al mismo tiempo identificar posibles opciones de herramientas de seguridad adaptativa que fortaleciera el modelo de seguridad de la organización. Una manera de llevarlo a cabo este objetivo es mediante pruebas de conceptos de herramientas de seguridad adaptativas en busca de identificar mejoras en el esquema de seguridad o identificar debilidades en función del malware que haya logrado evadir las barreras de protección convencionales.

Ejecutada la prueba de concepto con una de las herramientas más importantes se obtuvieron los siguientes resultados:

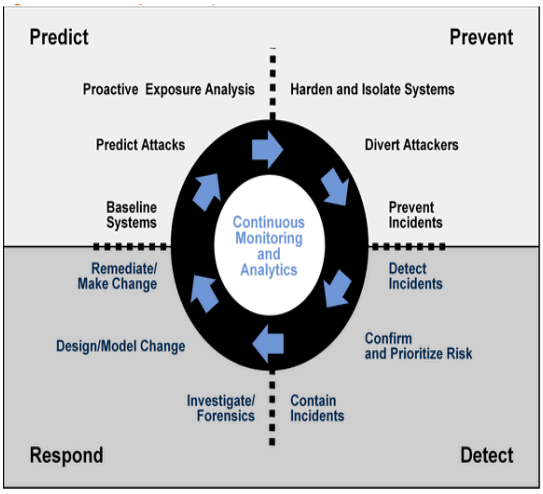
- Se encontró presencia de malware dentro de la organización, el cual estaba en varios computadores de la red interna de la organización.
- El malware no había sido detectado por las herramientas de seguridad convencionales implementadas por la empresa.
- El método de infección y propagación no está

determinado, posiblemente la fuente es por la implementación de equipos personales de los funcionarios o proveedores dentro de la red interna de la organización.
- No se logró determinar que el malware haya explotado vulnerabilidades adicionales o se haya presentado fuga de información.
- Lasa organización debe tomar en serio el riesgo que representan las APT.

V. COMO ENFRENTAR LAS AMENAZAS AVANZADAS PERSISTENTES

De acuerdo a un estudio realizado por Gartner en el año 2014, en el cual adicionalmente proponen un esquema de seguridad adaptativa que permite prepararse contra los tipos de ataques avanzados mediante una defensa integral en cuatro fases: prevenir, detectar, responder y predecir las cuales incluyen 12 capacidades claves que se observan en la siguiente figura:

Figura 2. Ciclo de la Arquitectura de Seguridad Adaptable



Fuente: Gartner (Febrero 2014)

La estrategia de defensa aplicada actualmente en la mayoría de las organizaciones está basada en la implementación de múltiples sistemas de protección desintegrados que no fueron diseñados para realizar investigaciones en profundidad. Por su parte los ataques cibernéticos avanzados se valen de operaciones meticulosas e integradas que incluyen un conjunto definido de técnicas de reconocimiento, infiltración y robo de datos teniendo la posibilidad de invertir altos recursos en el propósito de afectar el objetivo.

Mientras el grupo de seguridad se puede enfrentar a infinidad de alertas generadas continuamente, no tienen la posibilidad de investigar a fondo o correlacionar los datos encontrados en cada sistema. De acuerdo a lo anterior el criterio de seguridad frente a las amenazas persistentes avanzadas es obsoleto y continuamente fallido especialmente por la capacidad que tienen los atacantes para adaptarse a estos esquemas de seguridad. La implementación de sistemas de seguridad y análisis automatizados e integrados permiten a los analistas de seguridad eliminar lo superficial y orientarse a los ataques que realmente son importantes, la aplicación de estas herramientas reducen el tiempo de detección, aumentan la eficiencia y con ello detener los ataques y reforzar la seguridad contra posibles ataques futuros.
Para establecer una estrategia de defensa más robusta frente a las APT´s, se recomienda considerar los siguientes elementos:

- El malware realmente ya está en la organización.
- Es necesario re-imaginar la seguridad.
- Se requiere un giro hacia la seguridad adaptativa.
- Se requiere una defensa integrada End To End.
- Reconocer que la defensa en profundidad no es suficiente.

VI. CONCLUSIONES

Las siguientes conclusiones en función de la pregunta problemas y las hipótesis planteadas en el proyecto de investigación:

- El modelo de defensa en profundidad no riñe con los nuevos modelos de protección sugeridos (seguridad adaptativa) sino que le alimenta, esto es, no se puede implementar un modelo de seguridad adaptativa sin contar con mecanismos básicos de defensa perimetral.
- Si se implementará el modelo de defensa

adaptativo por si solo se estaría promoviendo un enfoque reactivo sin información para analizar y reduciendo los niveles de protección alcanzados.

- Es necesario fortalecer los controles aplicados sobre la infraestructura, así mismo se observa la importancia de fortalecer el control de cambios sobre la plataforma.

- Siendo la conexión de dispositivos personales de los empleados o de las terceras partes uno de los principales factores de riesgo para vulnerar la red corporativa, se deben fortalecer las políticas, procedimientos y controles en relación a ello.

VII. RECOMENDACIONES

Es necesario trabajar fuertemente en la concienciación y creación de cultura en seguridad de la información. Este reto ha sido un obstáculo grande en las organizaciones y se incrementa para lograr la compresión de las amenazas avanzadas persistentes.

- El modelo de Defensa en Profundidad es insuficiente frente a las APT pero no contar con él significa mayores niveles de exposición. La adquisición o implementación de soluciones de APT´s deben verse como la capa de detección y respuesta del modelo de Defensa en Profundidad.
- Dar el giro hacia la seguridad adaptativa significa más que adquirir soluciones APT´s. Se requiere fortalecer el modelo de Defensa en Profundidad y contar con equipo de respuesta a incidentes mucho mejor estructurados, entrenados y capacitados.

VIII. REFERENCIAS

[1] CISCO. SAFE Reference Guide. Cisco Validated Design. July 8, 2010.

[2] CISCO. DNS Best Practices, Network Protections, and Attack Identification.

[3] INFORMATION SYSTEMS SECURITY ARCHITECTURE PROFESSIONAL. Official (ISC)2 Guide To the ISSAP CBK. CRC Press. 2010.

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO - IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements.2013-

[5] ISACA. Business Model For Information Security.

[6] ISACA. E-Commerce Security: Securing The Network Perimeter, 2004.

[7] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Border Gateway Protocol Security. Special Publication 800-54. July 2007.

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Electronic authentication guideline NIST SP 800-63-2. August 2013.

[9] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to Intrusion Detection and Prevention Systems (IDPS). Special Publication 800-94. February 2007.

[10] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to IPsec VPNs. Special Publication 800-77 .December 2005.

[11] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to SSL VPNs. Special Publication 800-113. July 2008.

[12] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guidelines on Firewalls and Firewall Policy. Special Publication 800-41. September 2009.

[13] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cibersecurity, Version 1.0, February. 2014.

[14] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST 800 – 14 Generally Accepted Principles and Practices for Securing Information Technology Systems.

[15] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST 800 – 30 Risk Management Guide For Information Technology Systems.

[16] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Special publication 800-39, Managing information security risk, organization, misión and information systems, EEUU. 2011.

[17] MERCHÁN PATARROYO RAMIRO. Seminario Seguridad de la Información, Universidad de la Sábana.2014.

[18] STALLINGS WILLIAM Y BROWN LAWRIE. Computer Security, Principles and Practice, 3 Edition. Pearson Editorial, 2014.

[19] www.checkpoint.com/.

[20] www.fireeye.com/.

[21] http://www.gartner.com/technology/

[22] www8.hp.com/us/en/software-solutions/network-security/

[23] www.iboss.com/.

[24] www.sans.org.

[25] www.verint.com.

Autores

Ramiro Merchan Patarroyo.
Ingeniero de Sistemas.
Universidad Piloto de Colombia
2015

Diego Alejandro Carrillo.
Ingeniero de Sistemas.
Universidad Piloto de Colombia
2015