Framework de Seguridad informática para mitigar la fuga de información ocasionada por APT proveniente de correo electrónico, en los activos de información del sector hospitalario en Colombia.

Gloria Amparo Lora Patiño
Yexid Montenegro

Instituto Tecnológico Metropolitano
Facultad Ingeniería
Medellín, Colombia
2018

Framework de Seguridad informática para mitigar la fuga de información ocasionada por APT proveniente de correo electrónico, en los activos de información del sector hospitalario en Colombia.

Gloria Amparo Lora Patiño
Yexid Montenegro

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:
Magister en Seguridad Informática

Directores:
Magister Milton Javier Mateus
Doctora Paula Andrea Rodríguez

Línea de Investigación: Ciencias de la Computación
Instituto Tecnológico Metropolitano
Facultad de Ingeniería
Medellín, Colombia
2018

Dedicatoria

Le dedicamos esta tesis a nuestras familias por todo su apoyo y ayuda durante este proceso, en especial a mi esposa Milena Pantoja, a Hensen Montenegro y Tailini Montenegro que desde el cielo nos ilumina, y a Mateo Giraldo Lora. Quiénes con sacrificio de no ver a sus padres muchos fines de semana, hizo posible este sueño.

Agradecimientos

Expresamos nuestra total gratitud a nuestro director inicial al Magister Javier Mauricio Duran por sus contribuciones técnicas y humanas invaluables a esta tesis; además por su acompañamiento, amistad incondicional, confianza y apoyo.

A los directores que por razones del azar continuaron con nosotros el Magister Milton Javier Mateus y la Doctora Paula Andrea Rodríguez, que siguieron contribuyendo desde la parte metodológica y técnica e hicieron con sus aportes, evaluaciones y contribuciones al trabajo.

Agradecimientos a nuestros compañeros de cohorte a quienes agradecemos también por su amistad y confianza, principalmente por su acompañamiento académico y personal para cumplir con el desarrollo de esta tesis: Juan Carlos Balvin, Hernán Alonso Bernal, Carlos Augusto Ruiz, Cesar Augusto Ríos, Jorge Mario Aristizábal, Johan Javier Urrego, Elvy Johanny Chacón Navas, Andrés Felipe Osorio, quienes en cada una de las exposiciones hicieron aportes valiosos a esta tesis.

A los diferentes docentes de cada uno de los módulos de la maestría, por sus conocimientos técnicos y por su calidad humana.

Introducción

En especial también yo Gloria Amparo Lora Patiño quiero agradecer a grandes compañeros que se cruzaron en este proceso Manuel Alejandro Ramírez Timana, Juan David Grajales, Juan Carlos Balvin, Elvy Johanny Chacón Navas, Javier Mauricio Duran y Yexid Montenegro por su amistad, apoyo y ayuda prestada en todos estos años, su presencia fue muy especial e importante e hicieron parte fundamental del desarrollo de esta tesis. Un bello recuerdo me llevo de ellos.

Resumen

Introducción

El sector salud no cuenta con controles para detectar y detener las amenazas persistentes avanzadas (APT). Muchas organizaciones del sector dicen que al ser víctima de este tipo de amenaza, el resultado es el robo de información personal muy sensible. Para minimizar los

riesgos de que dichas amenazas se materialicen y puedan afectar el sector hospitalario de Colombia con posibles fugas de información, en este proyecto de grado, se propuso un Framework de seguridad informática orientada al sector hospitalario que permite mitigar la fuga de información ocasionada por APT que se propaga a través de correo electrónico. Para lo cual, se cuenta con una estrategia de clasificación de activos, un conjunto de buenas prácticas y un conjunto de herramientas, artefactos y aspectos metodológicos que permitan mitigar dichas amenazas.

Para lograrlo se realizó una guía de identificación de los activos de información sensibles del sector salud, que sean susceptibles a fuga de información, luego de ello se identífico y modeló un conjunto de amanezas para determinar el modus operandi de las APT provenientes de correo electrónico, para ello se hizo una propuesta de buenas prácticas y herramientas en cada una de las fases del ciclo vida de las amenazas persistentes avanzadas. Todo lo anterior para la mitigación de posibles fugas de información, por último se muestran los artefactos del marco de trabajo y su respectivo levantamiento de pruebas realizado a los activos de una entidad hospitalaria en Colombia. El resultado de este proyecto de grado es un framework de seguridad informática que ayuda a la mitigación de la fuga de información ocasionada por APT proveniente de correo electrónico, en los activos de información del sector mencionado anteriormente, el cual incluye una serie de procedimientos para la detección de amenazas y conjunto de riesgos que se asocian a buenas prácticas, herramientas que fueron probadas para demostrar la efectividad y mitigar el nivel de fuga en los activos.

Así mismo, las entidades hospitalarias podrán replicar el uso de este framework, el cual fué diseñado bajo el concepto de DLP, como una herramienta de control humano más no una herramienta técnica como las que se suele usar comercialmente.

Abstract

Introducción

The sector does not have controls to detect and stop advanced persistent threats (APT). Many organizations in the sector say that the service is very easy. To minimize the risks of being denounced materialize and establish in the hospital sector of Colombia with possible

information errors, in this degree project, a computer security framework aimed at the hospital sector that mitigates the leakage of information is proposed caused by APT that spreads via email. For whatever it is, there is an asset classification strategy, a set of good practices and a set of tools, artifacts and methodological aspects that mitigate these threats. To achieve this, a guide was created to identify the assets of the sensitive information of the health sector, which are susceptible to the leakage of information, after which a group of people are identified and modeled to determine the mode of operation of the health sector. APT from e-mail, for this a proposal of good practices and tools was made in each of the phases of the life cycle of advanced persistent responses. All of the above for the mitigation of possible information failures, finally, the artifacts of the framework and their respective survey of the tests performed in a hospital entity in Colombia are shown. The result of this degree project is a computer security framework that helps mitigate the leakage of information caused by APT from email, in the information assets of the aforementioned sector, which includes a series of procedures for the The detection of risks and the set of risks associated with good practices.

Likewise, the hospital entities will be able to replicate the use of this framework, which was designed under the concept of DLP, as a human control tool but not a technical tool such as those that are usually used commercially.

Palabras clave: Riesgo, Amenaza, Vulnerabilidad, Salud, Framework, Fuga, APT

Contenido

Introducción

1
2

Introducción

Lista de ilustracións

Pág.

Introducción

Introducción

LISTA DE TABLAS

PÁG.

Introducción

2
2

Introducción

Introducción

Introducción

Introducción

El proyecto de grado presenta de manera secuencial el cumplimiento de los objetivos propuestos los cuales se enuncian a continuación. **Objetivo General**: Proponer un marco de trabajo de seguridad informática para el sector hospitalario en Colombia que contribuya a la mitigación de la fuga de información ocasionada por APT, proveniente de correo electrónico.

Específicos: 1) Proponer una estrategia para identificar y clasificar los activos de información sensibles del sector hospitalario, que sean susceptibles a fuga de información ocasionada por APT, proveniente de correo electrónico, 2) definir un conjunto de políticas y buenas prácticas que permitan mitigar la fuga de información en los activos sensibles del sector hospitalario, en cada una de las fases del ciclo de vida del APT, 3) caracterizar un kit de herramientas que permita la ejecución de las buenas prácticas propuestas en el framework para la mitigación de fuga de información en el sector hospitalario, 4) definir un conjunto de artefactos, herramientas y aspectos metodológicos para el framework propuesto, que permita la mitigación de fuga de información proveniente de correo electrónico cuyo vector de infección sea mediante correo electrónico y por ultimo 5) evaluar el grado de efectividad del framework propuesto para la mitigación de fuga de información proveniente de correo electrónico cuyo vector de infección sea mediante correo electrónico.

Todo lo que se planteao anteriormente, se enfoca en dar solución a las amenazas que se han venido presentadon a las infraestructuras críticas nacionales y que son una realidad las cuales presentan una tendencia creciente. En 2015, la OEA y Trend Micro llevaron a cabo una encuesta entre los jefes de seguridad de infraestructuras críticas nacionales, donde hicieron algunos hallazgos: El 53% de los encuestados había observado un incremento de los incidentes en sus sistemas de cómputo durante el 2014, y el 76% de los encuestados respondió, que dichos incidentes contra las infraestructuras críticas nacionales se han vuelto más sofisticados (Departamento Nacional de Planeación, 2016); Colombia pasó de gestionar un total de 4.640 incidentes digitales en 2014 a un total de 7.323 en 2015. La gran mayoría de este tipo de ataques preocupa por la efectividad de los mismos y muchas veces se dificulta la detección de estos de forma oportuna.

El tema de robo de información o fuga tienen un alto impacto en las organizaciones de la salud, dado la relevancia, en términos de riesgos, que esto supone, es así como para america

del sur según estudios realizados (PwC, 2018) el 48% de los encuestados (en su mayoría empresa) indican la importancia sobre amenazas asociadas al compromiso de datos confidenciales, lo que supone un gran reto para la región, esto, considerando que en

Colombia la implementación y seguimiento de la ley 1581 sobre la regulación de habeas data es una obligación en las empresas, considerando un factor fundamental la protección de los datos en el sector Salud.

Por otro lado, acorde al ministerio de las TIC, en Colombia 83% de las empresas no poseen o tienen falencias en la creación o uso de procedimientos para abordar los incidentes de seguridad asociado a la violación de las políticas de seguridad (MinTIC, 2018), en ese mismo sentido, es preocupante como en el sector salud un alto porcentaje de las entidades desconocen la cantidad de incidentes de seguridad que se les presenta en sus corporaciones (ACIS, 2018), un valor preocupante teniendo en cuenta la misma responsabilidad que se tiene, por ejemplo en el cuidado de las histórias clínicas, para con los pacientes.

Así mismo, las inversiones en seguridad no son importantes, lo que sugiere una brecha cada vez más grande en cuanto a protección de información, siendo el sector salud uno de los sectores con menor inversión en temas de seguridad en comparación con el sector financiero o incluso el de consultoria especializada (ACIS, 2018). La importancia de contar con inversiones y profesionales calificados, generan confianza y reducción de riesgos que puedan afectar la disponibilidad, confidencialidad y/o integridad.

Por eso la importancia de contar con elementos administrativos y técnicos que apoyen la gestión en el sector salud, y máxime cuando las inversiones no se enfocan a la seguridad de la información, se proponen métodos o framework que identifiquen y/o reduzcan los niveles de exposición.

Para éste proyecto, la identificación y control de posible fuga de información se hace a través del framework desarrollado, que funciona como una guía estratégica de buenas prácticas de gobierno de TI y gestión de TI, que describe las acciones a seguir y que pueden servir como insumo de mejores prácticas de su aplicación en el sector salud.

Al hablar de fuga de información se hace necesario introducir diferentes elementos y estrategias asociados a la identificación y prevención de éste tipo de riesgos, tales como los DLP (Data Loss Prevention); estos son soluciones que permiten monitorizar, analizar y controlar los medios de entrada y salida de información, como el correo electroncio, web, mensajería instantánea, USB entre otros con el fin de proteger los datos confidenciales de la empresa y asegurar el cumplimiento de las políticas de seguridad; en este proyecto de grado

no se propone una herramienta técnica DLP, si no que toma dicho concepto como una estrategia que mitiga la fuga de información orientado al control por parte del usuario, que

una herramienta a nivel técnico; que trata de minimizar la fugas de datos debido a errores por falta de controles a nivel de usuarios.

El trabajo de grado inicia con el marco teórico, el estado del arte que dan soporte al desarrollo de la propuesta. Luego se continua mostrando la metodología usada para dar cumplimiento a los objetivos, seguido de esta, se muestran los resultados obtenidos en cada uno de los objetivos propuestos. Así mismo se desarrolla en cada capítulo el estudio para la creación del framework (marco de trabajo), la ejecución de este y los resultados de prueba generados a partir de un caso real, que permite identificar las amenazas y riesgos a los que están expuestos los activos del sector salud en Colombia.

El framework que se propuso es la recopilación de buenas prácticas existentes en el sector de la seguridad de la información y de la informática, puesto que a través de este se definieron los artefactos, herramientas y aspectos metodológicos que permitirán al administrador del sector hospitalario tomar medidas, mejores prácticas de gobierno de TI y gestión de TI, que le permitan mitigar la fuga de información ocasionada por APT proveniente de correo electrónico, por último se entregan conclusiones, recomendaciones y trabajo futuro en el desarrollo de la tesis.

Introducción

1.Marco Teórico y Estado del Arte

1.1.Fuga de información

En el campo de seguridad informática, la fuga información es la extracción no autorizada de información segura, e incluyen la divulgación de información y pérdida de datos, por medio de correo electrónico, P2P, transmisiones cifradas, infecciones de malware en dispositivos de extremo, smartphones y reproductores MP3, ingeniería social, etc. Así mismo en el código penal colombiano se define como "la revelación dolosa de informaciones concernientes a la vida personal y familiar, o del patrimonio económico individual, que posean personas o entidades autorizadas en sus bases de datos. Estos sucesos pueden generarse por: acción intencional (Supresión, robo o extracción de información, sabotaje, gusanos, virus, hackers), acciones no intencionales: eliminación o pérdida accidental de datos, mala administración de la información, errores: fallas de energía, de hardware, de software. Corrupción de datos y desastres Naturales. (Ministerio de las TIC. 2016)

Soluciones para prevenir perdida de información

Existen muchas soluciones técnicas que se enfocan a la prevención de fuga de información, los cuales se centran en identificarla y categorizarla. Muchas de estas soluciones tienen sentido en el concepto, pero en la práctica existen varios obstáculos.

La información esta dispersada, desorganizada y en grandes volúmenes, y clasificarla de forma comprensiva es una tarea demasiado tediosa y consume muchos recursos, tanto materiales como en tiempo.

Los productos de prevención de fuga de información son relativamente nuevos y pueden presentar incidentes que frecuentemente son "falsos positivos".

Los usuarios se resisten al cambio, ya que considerarán que estos agentes disminuyen la capacidad de sus herramientas.

Complejidad: Implementar unas políticas comprensibles y viables mitiguen la fuga de información puede encaminar a la organización a hacia buenas prácticas, pero se necesita que se involucre todos los empleados.

Enfoque incorrecto: La mayoría de organizaciones se enfocan en fuga de información intencional, pero esta es difícil de evitar. Ya que las personas deliberadamente podrían modificar archivos y saltar la detección, así mismo las personas comparten información por

Introducción

canales inapropiados si no existen políticas claras, planes de capacitación de personal y guias de buenas prácticas que permitan mitigar la fuga.

1.2. DLP (Data Loss Prevention)

Es una práctica de detectar evitando que los datos confidenciales sean "filtrados" fuera de los límites de una organización por personas no autorizadas. Los datos pueden ser eliminados física o lógicamente de la organización ya sea intencionalmente o no**.** También se define como una herramienta que traen los sistemas operativos para prevenir que se ejecuten datos que pongan en riesgo el sistema operativo y permite hacer hardening. (Cruz, 2010). En algunos casos es necesario consultar con profesionales con experiencia en regulación local, antes de implementar procesos DLP para garantizar el cumplimiento de las regulaciones de privacidad locales de cada pais. Es por ello que el framework que se propone en está tesis trabaja bajo el concepto DLP, debido a que tiene como finalidad dar lineamientos para cubrir algunos aspectos en una entidad hospitalaria tales como:
1.Prevenir la divulgación intencional o no intencional de datos confidenciales en reposo, en uso o en moción a partes no autorizadas, 2. Mantener seguridad adecuada y proporcionar usabilidad, proteger los datos del cliente y la imagen de la entidad hospitalaria, 3 .Proteger información personal identificable y propiedad intelectual, 4. Reducir el riesgo y el costos ocasionados por eventos indeseados.

La estrategia que se implementará con un enfoque DLP, tiene una visión holística para garantizar que la combinación de controles empleados esté orientada para proteger los datos más sensibles que posee la organización hospitalaria que es el objetivo principal a satisfacer haciendo uso de mejores prácticas de gobierno de TI y gestión de TI.

1.3 Framework

Se define como conjunto estandarizado de conceptos, buenas prácticas y criterios que se enfoca en un problema particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar(Matalobos, 2009).

El framework que se propone está orientado a:

- A identificar los activos de información del sector salud, sensibles a fuga de información, a causa de amenazas persistentes avanzadas.
- Dar orientación para proteger los activos sensibles a fuga del sector hospitalario

Introducción

- Es un framework construido a partir de una recopilación de buenas prácticas de los framework existentes en cuanto a seguridad de la información y de la informática.
- Suministrara herramientas técnicas, administrativas y físicas que permitan mitigar la fuga de información a causa de las amenazas avanzadas persistentes.

- Es una herramienta mas de control a nivel humano mas que técnico.

1.4. Framework de seguridad de la información

La información, es uno de los principales activos de cualquier organización, para el normal funcionamiento y la consecución de sus objetivos, según la política de la empresa, debido a esto las empresas y organizaciones necesitan proteger su información, para asegurarse que esta sea fiable, a la hora de gestionar grandes volúmenes de información (Sánchez et al., 2014)(MINTIC, 2016e). La seguridad de la información, es el proceso mediante el cual la empresa mantiene y alcanza unos niveles apropiados de confidencialidad, integridad, disponibilidad y autenticidad, a lo largo del tiempo diversas organizaciones del orden nacional e internacional se han dedicado a la definición estándares y normas que apoyan en diferente medida el cumplimiento de los requerimientos mencionados anteriormente; a continuación se especifican los de mayor utilización y que fueron tomados como base para el framework propuesto; desde ese punto de vista existen varios, que garantizan los niveles de seguridad a nivel de confidencialidad, integridad, disponibilidad y autenticidad entre ellos están:

1.4.1. Norma ISO 27001:2013.

Dedicada a la seguridad de la información; específica los ítems para la seguridad de la información, más no las directrices para ello, el proceso se describe en los siguientes ítems: Estructura para la seguridad de la información, lo que tiene que ver con terceros, el control de acceso, adquisición y desarrollo de los sistemas de información, sirviendo de apoyo para el proyecto en cuanto a lo que ISO 27000 puede ofrecer para el proyecto (Lopez y Ruiz, 2005):

- El alcance que tendrá el SGSI sobre los procesos de la entidad hospitalaria

- La política general de seguridad de la información

- La identificación y valoración de los activos de la información.

- Los riesgos a los cuales los activos identificados se encuentran expuestos.

Introducción

- La selección de los controles para mitigar los riesgos que se han detectado.

1.4.2. ISO 27799: 2016 e ISO / IEC 27002.

Al ser tomadas en conjunto, definen lo que se requiere en términos de seguridad de la información en el sector hospitalario. La norma ISO 27799 de 2016, es neutra desde el punto de vista tecnológico. Esta neutralidad es con respecto a la implementación de tecnologías. Proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluyendo la selección, implementación y administración de controles teniendo en cuenta el ambiente de riesgos de seguridad de la información de la organización, en un entorno donde las amenazas y vulnerabilidades únicas, debe considerarse con especial atención (ISO, 2016).

1.4.3. ISO 31000.

Es la norma que brinda los principios y las directrices genéricas sobre la gestión del riesgo. Esta norma se puede aplicar durante toda la duración de una organización y a un amplio rango de actividades, incluyendo estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

Esta norma se puede aplicar a cualquier tipo de riesgo, cualquiera sea su naturaleza, bien sea que tenga consecuencias positivas o negativas.

El numeral 5 contempla lo siguiente: Comunicación y consulta (5,2), Establecimiento del contexto (5.3), Valoración del Riesgo (5.4), Identificación del Riesgo (5.4.2), Análisis del Riesgo (5.4.3), Evaluación del riesgo (5.4.4), Tratamiento del riesgo (5.5), Monitoreo y revisión (5.6) (Ramírez & Ortiz, 2011).

1.4.4. ISO 20000.

Es el primer conjunto de normativa internacional específica para la gestión de los servicios basados en las Tecnologías de la Información (TI). Introduce en la organización de las TI una forma de trabajo metódica, integrada y orientada a los procesos, haciendo especial énfasis en garantizar la calidad del servicio a los distintos clientes de las TI. Además, articulan su implantación con un sistema de gestión específico, que incorpora la disciplina y el rigor de ISO 9000 en la implantación del modelo de trabajo en las TI. Los principios que interesan

Introducción

de ISO 20000 son los siguientes: procesos de la provisión del servicio, procesos de resolución, antecedentes, gestión del incidente, gestión del problema, procesos de control.(Matalobos, 2009) .

1.4.5. COBIT.

Es el marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa. Este documento contiene los 5 principios de COBIT 5 y define los 7 catalizadores que componen el marco, los que hacen referencia a las políticas de seguridad son: APO13 Gestionar la seguridad, A9012 Gestionar el riesgo, PO9 Evaluar y gestionar los riesgos de TI (Definir plan estratégico, gestionar los proyectos, garantizar la continuidad del negocio, garantizar la seguridad de los sistemas, proporcionar el gobierno de TI) (ISACA, 2016).

1.4.6. ITIL.

Conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL asegura una gestión de servicios de IT eficiente, gracias al control y una posterior la mejora continua del servicio. Actualmente hay varias versiones ITIL V.2 e ITIL V.3. Ambas se centran en Mejora continua del servicio con alineamiento de Estrategia del Servicio, Diseño del Servicio, Transición del servicio y Operación del servicio (Matalobos, 2009).

1.4.7. OCTAVE

Es un modelo para la creación de análisis de riesgos desarrollado por la universidad de Carnegie Mellon, es un conjunto de criterios (principios, atributos y resultados) a partir de los cuales se pueden desarrollar diversas metodologías. Posee tres versiones, pero la ajustada para el análisis de riesgos es OCTAVE ALLEGRO, con un enfoque en los activos de información, en oposición al enfoque en los recursos de información. OCTAVE ALLEGRO contempla las siguientes fases:

FASE 1: Establecer dirección: establecer los criterios de valoración de los riesgos

FASE 2: Perfilar activos: desarrollar perfiles de activos de información e identificar los recursos de información.

Introducción

FASE 3: Identificar amenazas: identificar las áreas de interés para el análisis e identificar escenarios de amenazas.

FASE 4: Identificar y mitigar los riesgos: identificar riesgos, analizar riesgos y seleccionar enfoque de mitigación.(Caralli, Stevens, Young, & Wilson, 2007).

1.4.8. MAGERIT.

Fue creada por el Consejo superior de administración electrónica y pública. Su versión más reciente es la 2.0 publicada en 2006. Es una metodología abierta, de uso muy extendido en el ámbito español. Dispone de una herramienta de soporte llamada PILAR II, de uso gratuito para la administración pública española y comercial para las organizaciones privadas. Consta de tres volúmenes el volumen I es el método, el volumen II es el catálogo de los elementos, complementa diversos inventarios de utilidad en la aplicación de la metodología tales como tipos de activos, dimensiones y criterios de valoración, amenazas y salvaguardas; el volumen III son las guías técnicas; proporciona algunas técnicas a utilizar en las distintas fases del análisis de riesgos las técnicas que recoge son:

Técnicas específicas para el análisis de riesgos (Análisis mediante tablas, análisis algorítmico, árboles de ataque).

Técnicas generales (Análisis coste beneficio, diagrama de flujos de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo y valoración Delphi).(Ministerio de Hacienda y Administraciones Públicas, Centro Criptológico Nacional, 2012).

1.4.9. NIST SP 800-30.

Hace referencia a los controles de seguridad recomendados para los sistemas de organizaciones de información del gobierno federal de los estados unidos. Para el análisis de riesgos realiza los siguientes pasos:

a. Caracterización de sistemas, b. Identificación de amenazas, c. Identificación de vulnerabilidades, d. Análisis de controles, e. Determinación de probabilidades, f. Análisis de impacto, g. Determinación del riesgo, h. Recomendación de controles, i. Documentación de resultados.

Para la gestión del riesgo, hace referencia a los siguientes pasos: a. Priorización de las acciones, b. Evaluación de opciones controles recomendados, c. Análisis costo beneficio, d.

Introducción

Selección de controles, e. Desarrollo de plan de implantación de salvaguardas, f. Implantación de controles seleccionados (Matalobos, 2009).

1.4.10. SOMAP

Está compuesto por una organización sin ánimo de lucro cuyo objetivo es desarrollar proyectos Open Source, relacionados con la gestión de la información.

Posee en marcha 3 proyectos:

- Open Governance, Risk Compliance Maturity Management Methodology la cual contiene: cumplimiento, gestión de activos y categorización, medición y documentación del cumplimiento y reportes y evaluación.
- Open Risk Model Repository (ORIMOR) contiene una base de datos que da soporte al marco de referencia y a la herramienta. Contiene repositorios tales como:
  Tipos de activos y dependencias entre ellos, vulnerabilidades, salvaguardas, relación entre activos y vulnerabilidades, cuestionarios.
- Open Risk & Compliance Framework and tool (ORICO) herramientas que dan soporte al modelo. Actualmente en versión de prueba (Matalobos, 2009).

1.4.11. EBIOS.

Está dedicada a los administradores, permite apreciar y valorar los riesgos relativos a la seguridad de los sistemas de información, también posibilita la comunicación dentro del organismo y también con los asociados para contribuir al proceso de la gestión de los riesgos, posee una herramienta Open Source (Direction centrale de la sécurité de systèmes d'information, 2003).

1.4.12. HIPPA.

Es la ley de Portabilidad y responsabilidad Médica del gobierno de los Estados Unidos es la ley que tiene como prioridad la privacidad y seguridad de la información médica. Es una estándar que ofrece controles administrativos, físicos, técnicos, requerimientos de la organización hospitalaria al igual que políticas y procedimientos. Estos controles permiten evaluar el cumplimiento de las políticas de un dominio, detectar no conformidades y facilitar la detección de acceso, eliminación y modificación de información protegida (X. Chen, Zhang, Wu, & Han, 2005)

Introducción

1.5. Framework Orientados al sector salud

Los framework del sector Salud permiten a estos fortalecer los sistemas de información en general y establecer niveles de protección para que esta sea completa, eficiente, de calidad y ante todo disponible para el personal y los procesos que lo requieran.

En la tabla 1 se presenta un resumen los framework del sector salud, explicando su contenido, proceso y contexto, son framework orientados a proteger la historia clínica, el acceso a la información, confidencialidad y protección de la información:

Tabla Resumen de frameworks del sector salud

Nombre del Framework	Contenido	Procesos	Contexto
Marco de seguridad para portátiles NFC Mobile Based Health Record System	Es un framework que proporciona control de acceso basado en RBAC con acceso selectivo a lectura y escritura.	Los datos deben de estar cifrados para el permitir el acceso de personal solo autorizado. La técnica de cifrado de claves públicas tradicional requiere claves diferentes para el cifrado y el descifrado, pero implica la administración de claves complejas cuando un grupo de usuarios comparte la clave de descifrado, usa el cifrado basado en atributos. El marco de trabajo consta de un esquema CP-ABE basado en proxy el cual utiliza para RBAC con acceso selectivo de lectura y escritura a varias secciones de la tarjeta de salud y proporciona confidencialidad, integridad y privacidad del paciente. El almacenamiento se realiza en credenciales en suplentes como TEE Trustzone del procesador ARM o de alta velocidad. Usa en su implementación esquemas CP-ABE mejorados para la revocación escalable de usuarios Fuente:(Sethia, Gupta, & Saran, n.d.)	Es un sistema que proporciona al médico y al usuario tener un acceso a la historia clínica.
Un diseño del marco de seguridad para la privacidad de datos En el Sistema de Salud Electrónica utilizando el Servicio Web	Es un framework para la privacidad de datos en el sistema de salud electrónica basado en la arquitectura de servicios web	La información electrónica del paciente se almacena en la nube en varios servidores de terceros usando la encriptación, usando un framework de seguridad para datos. Estos datos pueden ser accedidos a través de un servicio web, aplicaciones web y aplicaciones de escritorio. El procedimiento incluye el uso de aplicaciones web sencillas, servicios web construidos junto con la base de datos como almacenamiento de datos. El robo de información por un tercero aún está latente, porque no se garantiza que la encriptación garantice la seguridad en un 100%. Fuente: (Thiranant, Sain, & Lee, n.d.)	El acceso a datos médicos electrónicos por parte de pacientes, médicos, enfermeras y cada uno de acuerdo a su perfil, garantizando que no haya ingreso por parte de un tercero.
Marco de autorización centrado en el paciente para compartir registros de salud electrónicos	Framework para el control de acceso que soporta el intercambio selectivo y centrado en el paciente.	Es un prototipo infoshare que utiliza en el mecanismo de consentimiento electrónico para permitir el intercambio de información entre diferentes entidades. Se propone registros electrónicos médicos con diferentes niveles de granularidad con	Es un marco de trabajo centrado en el paciente en el cual se usa varios niveles de granularidad, usando la protección de la privacidad.

Introducción

		control de acceso, integrando políticas de control de acceso al igual que mecanismo de identificación para procurar que solo acceda a la información el responsable. Fuente(Jin, Ahn, Hu, Covington, & Zhang, 2009)	

Diseño de un sistema de red de salud electrónica seguro	Se propone un sistema seguro de red e-salud; es una arquitectura que reducirá significativamente el riesgo de fugas de datos y el robo de datos, con un mínimo coste adicional o retardo en la red.	Esta arquitectura es dependiente de la aplicación cliente y garantiza el acceso autorizado a los registros de salud mediante el uso de un cliente seguro y un proceso de autenticación de 2 pasos más conocido como TOPT, también ofrece la posibilidad de la encriptación de datos tanto de pacientes, personal médico y personal de TI; esto quiere decir utilizar más los niveles de autenticación y evitar que el empleado use sus contraseñas y usuarios de otras redes sociales para autenticarse en el sistema y así evitar ataques de phishing. Fuente:(Luca, Brattstrom, & Morreale, 2016)	Protección de la confidencialidad y seguridad de la información del sector salud tanto de pacientes, médicos como del personal administrativo y así ayudar al sector hospitalario a controlar los gastos administrativos, por demandas de pacientes al ver expuestos sus datos a un tercero.
Mejora del marco de salud electrónica para la seguridad y la privacidad en el sistema de salud	Es un marco de trabajo que propone técnicas de cifrado para la protección de la información clínica del paciente.	Es un marco de trabajo que propone: - Control de acceso centrado en el paciente - Privacidad del paciente - Altamente escalable de acuerdo a las necesidades. - Punto de contacto único para mayor autenticación y autorización. - Evitar las vulnerabilidades y las amenazas tales como hombre en el medio, denegación de servicios.	Es un marco de trabajo que ha propuesto una técnica de cifrado MA-ABE. Esta técnica ayuda a lograr el control de acceso, al igual que, aumenta la posibilidad de evitar los ataques ocasionados por intrusos. Al igual también se propone el uso de la técnica CP-ABE.
Marco híbrido para la prevención y detección de la pérdida de datos	Es una técnica de prevención basada en reglas, la cual bloquea transacciones que han sido marcadas como sospechosas.	Para evitar la pérdida de datos a las cuales se ven expuestas muchas de las empresas de hoy en día , se utiliza patrones ya previamente identificados, usando el concepto de firmas, las cuales proporcionan la identificación precisa de los ataques en la detección de falsos positivos, puesto que se hace un seguimientos a patrones de conductas poco usuales los cuales permiten su detección, de esta manera proporcionan la capacidad de reducir la propagación de la fuga de datos y el esfuerzo que a veces requiere el usuario para garantizar su protección (Costante, Fauri, Etalle, Hartog, & Zannone, 2015)	Prevención y detección de pérdida de datos usando reglas predefinidas.

Tabla 1.Frameworks orientados al sector salud. Fuente de elaboración propia.

De acuerdo a la revisión de literatura de marcos de seguridad orientados al sector salud, se evidencia que la gran mayoría se centran en la protección de datos tales como: la historia clínica que en gran medida es la razón de ser del servicio hospitalario y la protección con técnicas de cifrado, también proponen procesos de autenticación para garantizar la integridad de los datos que allí reposan.

Introducción

Framework de seguridad para detección de APT

Se han propuesto algunos marcos para mejorar la seguridad en los sistemas frente a ataques avanzados, entre los cuales sobresalen:

Marco para mejorar la seguridad en los centros de datos basados en SDN, el cual permite mejorar la seguridad en los centros de datos, basándose en redes definidas por software para integrar la capa de red con middleboxes de seguridad como los sistemas de prevención de intrusiones o firewall para bloquear los atacantes en el borde de la red (Ammar, Rizk, Abdel-Hamid, & Aboul-Seoud, 2016). Autores como Securitymatters, Fauri, Etalle, Den Hartog, & Zannone (2016), también proponen un marco híbrido para la prevención y detección de la pérdida de datos, mediante el uso de un motor basado en anomalías, el cual aprende automáticamente de un modelo de comportamiento normal del usuario, lo que le permite identificar cuando se realizan transacciones anómalas, mediante el uso de alertas para crear y actualizar automáticamente firmas de ataques basándose en reglas de prevención, bloquea transacciones marcadas previamente como maliciosas antes de que puedan causar algún daño.

Por otro lado, se proponen frameworks de seguridad mediante análisis big data, que a continuación se describen:

Gupta & Jyoti (2014), proponen un marco que combina diferentes técnicas, basado en el análisis de datos y la seguridad inteligente para apoyar a los analistas en la priorización de los host que tienen más probabilidades de verse comprometidos ante ataques APT. También se ha propuesto otro marco mediante análisis big data con hadoop para analizar ataques dirigidos a datos empresariales y mitigar con la implementación de seguridad, haciendo uso de análisis big data y proteger los datos de la empresa de forma eficiente (Marchetti, Guido, Pierazzi, & Colajanni, 2016). Además existe un estudio e investigación de la tecnología de detección de APT basada en una arquitectura de procesamiento big data, este marco incluye captura, procesamiento y análisis de las amenazas en la capa de aplicación. Al tiempo que el sistema puede detectar ataques APT conocidos y desconocidos y permite realizar análisis forense para APT (Shenwen, Yingbo, & Xiongjie, 2015). También Jia (2017), hizo un estudio sobre seguridad de la información de red basada en análisis big data que permite la protección contra APT, que integra las estrategias de defensa a profundidad para identificar posibles ataques APT.

Por último, en la Universidad Internacional de la Rioja, se han propuesto metodologías de Análisis de Malware, entre las que se destacan:

Introducción

Análisis de Malware caso de estudio de la Amenaza Avanzada Persistente (APT) Octubre Rojo propuesta por Abad-Aramburu (2015) y análisis de (APT) Poison Ivy (Por et al., 2016), que consisten en acciones iniciales, basadas en la creación de escenarios de prueba y obtención de la líneas base de la víctima, la clasificación, basado en la obtención de

información del APT, análisis estático y dinámico de código y análisis del comportamiento de acuerdo a la ejecución y estudio del comportamiento del código malicioso en tiempo real. Desde este punto de vista los frameworks existentes se basan en prevención, donde aplican técnicas basadas en el uso de firmas, en anomalías, análisis estático y dinámico que en la mayoría de los casos son incapaces de detectar ataques de día cero, así mismo presentan un incremento de falsos positivos, también se caracterizan por tener costos de operación altos. En fin, la gran mayoría están centrados en proteger la información de ataques tales como la ingeniería social, hombres en el medio y denegación de servicios, desconociendo que muchas de estas técnicas son el punto de partida de las amenazas persistentes avanzadas que es un tipo de ataque que puede afectar altamente la confidencialidad de la información y la prestación de servicios.

El marco de trabajo que se propone es la recopilación de un conjunto de buenas prácticas de seguridad y técnicas orientadas a proteger los activos de información importantes del sector hospitalario, que busca dar solución no solo a la historia clínica sino a cualquier tipo de información que reposa en los servicios hospitalarios.

1.7. Amenazas en el sector Salud

Uno de los factores que más preocupa, son las 26 denuncias presentadas en 2014 de incidentes, dentro de las cuales 12 estaban asociada a robo de hardware donde contenía información de pacientes sin cifrar, a Junio de 2015 el número de infracciones ha aumentado a 234, se considera que el valor económico de un registro médico puede ser más costoso que la información de una tarjeta de crédito (Raj, 2016), esto puede traer consigo el acceso a los datos tales como nombres, fechas de nacimiento, números de seguridad social, direcciones, números de teléfono, direcciones de correo electrónico, ingresos y empleo de la información. Otra preocupación es el acceso a los registros sin la verificación de privilegios de los empleados. El sistema de salud enfrenta tres tipos de amenazas: robo de datos, que se puede dar por accesos indebidos a la información, estafas a través de correos electrónicos y fuga de información que normalmente se da por exceso de privilegios de algunos empleados, para acceder a información privilegiada (Luca et al., 2016).

Introducción

1.7.1. Ataques

La ingeniería social: Es un método usado por los atacantes para obtener acceso a un sistema de forma ilegal, viéndose comprometida la confidencialidad de la información, en muchos casos los datos son robados. Una de las estadísticas afirma que alrededor del 60% de las

personas piensan que la fuga de datos involuntaria es la más importante (Xiangyu, Qiuyang, & Chandel, 2017). La ingeniería social también se puede definir también como la violación de la seguridad de una empresa engañando a las personas para que rompan procedimientos normales de seguridad. Por ejemplo, convencer a las personas a través del engaño para que entreguen información como identificación de usuario, contraseñas o directorios corporativos; es una técnica es usada por piratas informáticos donde por medios técnicos no han logrado acceder a un sistema (Ghafir, Prenosil, Alhejailan, & Hammoudeh, 2016).

Las amenazas se dividen en dos tipos: Intencional y no intencional. El 60% de las personas piensan que la fuga de datos involuntaria es la más importante. La amenaza interna involuntaria es aquella donde los empleados, socios y otras personas quienes autorizan de forma involuntaria el acceso a un sitio web o el acceso al software de la empresa.

La ingeniería social puede causar fuga de información la cual puede darse por dos categorías:

a. Físico: Corresponde a documentos físicos, perdida de portátiles, unidades de almacenamiento.
b. Virtual: Código malicioso, malware, spyware, ataques de correo electrónico de phishing.

Estos pueden ser ataques a:

a. Corto plazo: Se aplica cuando la información sustraída causa una mayor pérdida y daño a la compañía. El atacante no usa la información robada por mucho tiempo.
b. Lago plazo: El atacante explota una vulnerabilidad inicial para infiltrarse y atacar la empresa; lo que resulta en daños a intereses de la compañía.

Un atacante se poder valer de 3 formas para obtener la información:

a. Amenazas en Línea: Es la más propagada en este mundo electrónico donde se recibe y se transmite información corporativa. Se usa el correo electrónico, aplicaciones, gusanos y virus.
b. Amenazas telefónicas: Ya no son tan comunes.
c. Búsqueda en basura: Se hace a través de redes sociales, id corporativos entre otros.

Introducción

Las amenazas en línea se usan en la gran mayoría de los casos, valiéndose de correos electrónicos de *spear phishing* a menudo son el truco principal utilizado por los atacantes para acceder a las redes de la organización e implantar un APT.

La diferencia entre un Spear Phishin y un Phishing es que el primero es una estafa de correo electrónico dirigido a empresas u organizaciones con el fin de robar datos para fines maliciosos, algunas veces tratan de instalar malware en la computadora. Los correos electrónicos solo se envían a un pequeño grupo de personas cuidadosamente seleccionado. En la mayoría de los casos, contienen archivos adjuntos con software malicioso para proporcionar una herramienta de control remoto al atacante. Los exploits de día cero son una buena forma de instalar una puerta trasera a través de una vulnerabilidad existente (Xiangyu et al., 2017). (Krombholz, Hobel, Huber, & Weippl, 2015).

- **Suplantación De Identidad:** Es aquella acción por la que una persona o grupo de personas se hace pasar por otra(s) para llevar a cabo actividades de carácter ilegal, como por ejemplo realizar ataques contra terceras personas, esto es una acción cada vez más habitual en el contexto electrónico (Legalitas, 2016). En seguridad hacen referencia en seguridad de redes a la suplantación de identidad de un ordenador ajeno, el atacante se hace pasar por otro obteniendo acceso que en condiciones normales tendría restringido. Hay varios tipos entre ellos está el ARP SPOOFING, suplantación de identidad por falsificación de la tabla ARP (protocolo de resolución de direcciones), DNS SPOOFING, suplantación de identidad por el nombre de dominio, DHCP SPOOFING asigna parámetros IP falsos a las víctimas con fines malintencionados, cada uno de ellos tiene una forma de defensa muy particular, lo más importante es incorporar técnicas de defensa que mitiguen estas amenazas, puesto que este tipo de ataques origina perdida de confidencialidad, integridad y disponibilidad (Carlos, 2010). También hay otro tipo que es el correo falso, es cuando un atacante le envía un correo electrónico usando otra dirección de correo electrónico. Hace parecer que el mensaje es para ellos y engaña a las personas para que lo abran. La suplantación de correo electrónico es posible debido a SMTP (protocolo simple de transferencia de correo), se usa para enviar correo, no incluye un proceso de autenticación, logrando que este tipo de ataque puede estar manipulando al usuario fácilmente para divulgar la información fácilmente con solo dar un clic (S. Gupta, Singhal, & Kapoor, 2017).

Introducción

- **Identificar Activos Objetivo:** Este tipo de ataques se encarga de atacar navegadores, programas embebidos y códigos no protegidos. Entre los principales tenemos el SQL INJECTION, los ciberdelincuentes utilizan inyecciones de código SQL junto con secuencias de comandos entre sitios y programas maliciosos para introducirse en

sitios web y extraer datos o incrustar código malicioso, también los CSRF: (Cross-site request forgery o falsificación de petición en sitios cruzados) es un tipo de exploit malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía, Un ataque XSS (Cross Site Scripting) consiste en introducir código HTML o Javascript en las cajas de texto de formularios y si éstos no controlan los datos que se introducen, pueden hacer que ese código se ejecute en la web. Para la protección de este tipo de ataques es tratar de hacer códigos más seguros y de hacer suficientes pruebas antes de sacar un software a producción (amenaza web).

- **DDOS:** Es un ataque diseñado para confundir a las víctimas con tráfico y evitar que sus recursos de red funcionen correctamente, es una ataque que requiere una cantidad significativa de ancho de banda para que el ataque tenga éxito. Este tipo de ataque está dirigido a objetivos de todo tipo tanto de nivel doméstico como empresarial a veces el tráfico es de un tamaño tan insignificante que no es fácilmente detectable por alguna herramienta destinada para ello (Nazario, 2008).

Este tipo de ataques se centran especialmente a la capa de aplicación, debido a su fácil ejecución y detección difícil, es por ello por lo que los mecanismos de detección de ataques DDoS se han centrado en la mitigación. Es un ataque que se considera sofisticado porque imita las solicitudes de usuarios reales. Es por ello que en la capa de aplicación se deben analizar las características del usuario y así detectar si es un tráfico normal o anormal por ello es de importancia registrar las características de un usuario cuando interactúa con el sistema (Bravo & Mauricio, 2018).

El ataque de DDOS usan estos tipos de paquetes problemáticos que pueden ser de tipo TCP, UDP o ICMP porque el atacante debe seleccionar el tipo de tráfico antes de lanzar el ataque, el atacante debe seleccionar muy bien los agentes con que va a realizar el ataque para ello deben realizar un escaneo de red e identificar las vulnerabilidades de seguridad para instalar el software de ataque. Normalmente se esperan cambios en el tráfico durante la preparación del ataque. Las formas más comunes de ataque son consumo de recursos, destrucción de datos. Se recomienda estar preparado, identificarlo y hacer la fase de

Introducción

contención y recuperación, como también validar las entradas, comprobar el rendimiento del código y de las funciones (K. Lee, Kim, Kwon, Han, & Kim, 2008)

-**Escaneo De Vulnerabilidades:** En el escaneo de vulnerabilidades permite la identificación, análisis y reporte sistemático de las vulnerabilidades de seguridad técnica que terceros e

individuos no autorizados pueden usar para explotar y amenazar la confidencialidad, integridad y disponibilidad del negocio, los datos técnicos y la información. El escaneo de vulnerabilidades ayuda a una organización a identificar y remediar las vulnerabilidades dentro de su ambiente de TI antes de que los hackers y ladrones obtengan acceso a modificar o destruir información confidencial.

En general en el escaneo de vulnerabilidades se buscan componentes obsoletos de sistemas operativos y aplicaciones de software que tengan errores conocidos, muchas veces el atacante en este tipo de escaneo también puede encontrar errores de configuración, como el uso inadecuado de archivos compartidos y problemas similares.

Existen escaneo de vulnerabilidades basados en red que escanean todos los sistemas que se encuentran en la red, como también escaneo que se ejecuta en sistemas individuales con el aliciente que se pueden encontrar vulnerabilidades que pueden ser explotadas por alguien con acceso al sistema (Ira & Araceli, 2017).

-**Footprinting:** Consiste en la búsqueda de cualquier tipo de información pública, la cual se consigue con el desconocimiento del objetivo o porque haya sido publicada a conciencia. En este proceso se puede buscar y obtener desde direcciones IP de la organización objetivo, nombres y direcciones IP de servidores internos, cuentas de correo electrónicos de usuarios de la organización, información de dominios, impresoras, rutas internas, el estudio de los metadatos de los documentos públicos de una organización (Pablo, 2018)

-**Análisis De Vulnerabilidade**s: La vulnerabilidad es un punto débil en la seguridad de un sistema informático. A través de ésta se pueden presentar amenazas que pongan en peligro la confidencialidad e integridad de la información. El análisis de vulnerabilidades permite identificar el tipo y el nivel de cada vulnerabilidad según la necesidad.

-**Fuerza Bruta:** Son aquellos tipos de amenazas que exploran todo el espacio posible de claves para romper un sistema criptográfico. Los “ataques de diccionario”, que trabajan con una lista de posibles contraseñas: palabras de un diccionario en uno o varios idiomas, nombres comunes, nombres de localidades o accidentes geográficos, códigos postales, fechas del calendario. Esta técnica trata de averiguar la contraseña probando todas las

Introducción

combinaciones posibles. Es una de las técnicas más utilizados por los hacker para violentar la seguridad en las organizaciones y una manera de contrarrestarlos es a través del bloqueo del acceso a una cuenta después de varios intentos de inicio de sesión fallidos, generalmente tres (Rocío et al., 2017)(Baca, 2016).

-Backdoor: Es un tipo de troyano que permite acceder al sistema infectado y tener su control. De esta forma un atacante puede realizar acciones tales como eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas. Es una forma indocumentada de acceder a un programa. Es un riesgo para la seguridad potencial. Generalmente se ven integrados dentro de los troyanos, debido a que permiten esta usabilidad, un atacante puede conectarse siempre que quiere a los sistemas infectados, actualizar o cambiar los malware instalados para que realicen todo tipo de actividades o robar información sin que el usuario lo perciba (Josep, 2015).

-Phishing: Es un ataque donde el atacante manipula a las personas para obtener sus datos personales de manera fraudulenta, hace parte de los ataque de ingeniería social, cuyo objetivo principal es obtener de manera fraudulenta datos confidenciales de un usuario, aprovechando el uso que éste tiene en los servicios tecnológicos y que en la gran mayoría de estos no tienen medidas de seguridad para navegar en internet. En la actualidad los ataques de phishing son bastante sofisticados, debido a que usan mensajes de correo electrónico y falsos sitios Web, que suplantan perfectamente a los sitios originales (S. Gupta et al., 2017)(Tarazona, 2015).

-**Malware:** En términos generales es un programa informático que tiene efectos no deseados o maliciosos. Puede incluir virus, gusanos, troyanos y puertas traseras.
Utiliza herramientas de comunicación populares, tales como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse; también se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. En su gran mayoría el malware peligroso busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas (MINTIC, 2016e).

-**Ataques Zero Day:** Es un tipo de ataque contra equipos que se aprovecha de una vulnerabilidad desconocida por los usuarios y los programadores de las aplicaciones, de los cuales en ese momento no se tiene un parche que actualice o solucione dicha vulnerabilidad. Algunas veces se usan junto a los troyanos, rootkits, virus, gusanos y otros tipos de malware, para ayudarlos a propagarse e infectar más equipos. También se

Introducción

pueden encontrar escritas como “0day“, “zeroday” y “zero-day“. Pueden existir dos vulnerabilidades de día cero: La primera es una brecha en la seguridad del software y puede estar en un navegador o en una aplicación y la otra un exploit de día cero es un

ataque digital que se aprovecha de una vulnerabilidad de día cero para instalar software malicioso en un dispositivo (Myers, 2015).

-**Herramienta Maliciosa:** Las herramientas maliciosas son programas de software malicioso diseñadas para crear virus, gusanos o troyanos de manera automática, al realizar ataques DoS en servidores remotos, hackear otras computadoras y más. Son diseñados para crear virus, gusanos y troyanos y realizar ataques de denegación de servicio, en servidores y equipos. Su carga maliciosa solo se entrega bajo la orden directa del hacker (Lab, 2015).

-**Vulnerabilidades Conocidas:** Las vulnerabilidades conocidas son aquellas que comprometen la seguridad del sistema informático; entre estas encontramos:

a. Vulnerabilidad de desbordamiento de buffer: Esta sucede cuando un programa no controla la cantidad de datos que se copian en buffer llegando a un momento en que se sobrepase la capacidad del buffer y los bytes que sobran se almacenan en zonas de memoria adyacentes.

b. Vulnerabilidad de condición de carrera: Es aquella que ocurre si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad.

c. Vulnerabilidad de Cross Site Scripting (XSS): Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBSript o JavaScript en páginas web vistas por el usuario.

d. Vulnerabilidad de denegación del servicio: Una denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima como también sobrecarga de los recursos informáticos del sistema de la víctima.

e. Vulnerabilidad de ventanas engañosas (Window Spoofing): Son las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si se siguen se obtienen (Antivirus Mejor, 2016) datos del ordenador para luego realizar un ataque (Mifsud, 2012).

Introducción

-Escalar Privilegios: Es aquel acto de explotación de un error, fallo de diseño o configuración de una aplicación, dentro de un sistema operativo o aplicación, para conseguir acceso a recursos del sistema que normalmente están protegidos frente a una aplicación o usuario. Una aplicación con más privilegios de los necesarios según el rol

asignado; podría llevar a cabo acciones para las que no está autorizada y acceder a información para la cual no está autorizado. Existen dos tipos de escalonamiento:

A. Vertical: Es un tipo de ataque donde un atacante comienza con una cuenta de usuario comprometida y es capaz de ampliar o elevar los privilegios de usuario único que tiene cuando obtiene privilegios administrativos completos o "raíz", a tales ataques se les llama escalonamiento de privilegios vertical.

B. Horizontal: Es aquel tipo de ataque donde el atacante se aprovecha de un fallo de diseño, un usuario normal accede a contenido/permisos de otro usuario del mismo nivel y que está vetado al primero (Antivirus Mejor, 2016).

Esteganografia: Es la ocultación de información en un canal encubierto con el propósito de prevenir la detección de un mensaje oculto. Estudia el conjunto de técnicas cuyo fin es insertar información sensible dentro de otro archivo; a este se le denomina fichero contenedor. De esta forma, se consigue que la información pase inadvertida a terceros, de tal forma que sólo sea recuperada por un usuario legítimo que conozca un determinado algoritmo de extracción de la misma (Inteco, 2012).

Instalación Y Ejecución De Programas En Segundo Plano (Backgroud): Es usada para nombrar a todos aquellos procesos o rutinas de ejecución que se realizan en segundo plano.

1.8. Modo de operación de las APT más destacadas cuyo vector de ataque es el correo electrónico.

Una de las características de las amenazas persistentes avanzadas es el retraso promedio para la detección del de ataques, en el 2014 se demoraron 205 días y 229 días en el 2013. Los ataques más demorados en su detección fue Flame seis años de 2006 a 2012, Octubre Rojo 5 años de 2007 a 2012 (Id Messaoud, Guennoun, Wahbi, & Sadik, 2015). Los cuales se comportaban de la siguiente manera:

Introducción

1.8.1.Flame

Su objetivo consiste en robar archivos, capturar datos de pantalla, propagarse través de dispositivos USB y también tiene la capacidad de usar el vector de ataque correo y

deshabilitar la seguridad productos y explotar las vulnerabilidades conocidas o reparadas de Windows, para atacar la vulnerabilidad de los usuarios y sistemas (Antiy Labs, 2012).

1.8.2. Octubre Rojo

Hace uso de correos electrónicos dirigidos como vector de ataque. En este caso, el contenido de los correos electrónicos contenía una oferta de vehículos, una vez que el APT infectaba el equipo de la víctima, iniciaba las fases: Robo de datos de Celulares (iPhone, Nokia, etc.) y escanea la configuración de dispositivos de red (Cisco) (Abad, 2015).

También robaban información y ficheros de dispositivos extraíbles, enviaban los archivos robados a los servidores maliciosos mediante un canal de comunicación seguro. Tal y como confirma Kaspersky Lab (2013), el contenido (el malware adjuntado) fue reutilizado de otros ataques, así mismo los análisis realizados por kaspersky ponen en evidencia los exploits usados para acceder a los equipos que se sirven de las vulnerabilidades CVE-2009-3129 de Microsoft Excel, CVE-2010-33332, CVE-2012-0158 de Microsoft Word. Tras la infección de la víctima, el malware escaneaba información sobre la red interna de la organización objetivo, lo cual permitió conocer la topología de la red y la infraestructura, identificando los activos y sistemas críticos. Por último, se ejecutó la fase de propagación hacia sistemas identificados como críticos mediante la explotación de la vulnerabilidad conocida como MS08-06727.

1.8.3. APT Carbanak

Apareció en el año 2013 y en estos últimos años se ha registrado una serie de robos a bancos con pérdidas de más de 1 billón de dólares. Este APT afecta el servicio mediante mensajes phishing los cuales empiezan a robar toda la información almacenada en el equipo (Kaspersky, 2015). Todos los casos observados utilizan correos electrónicos de phishing de lanza con Microsoft Word 97-2003(.doc) o los archivos adjuntos archivos CPL. Los archivos con extensión .doc explotan las vulnerabilidades CVE 2012-0158, CVE-2013-3906 de Microsoft Office y de Microsoft Word (CVE-2014-1761).

Introducción

1.8.4. Operación Aurora

Según Holguín, Moreno y Merino (2013). Este tipo de APT utiliza el vector correo electrónico, valiéndose de la técnica Spear Phishing Attacks: similar al cuento del caballo de Troya. Cuando muchos empleados dieron clic provocó que dentro de sus computadoras se

ejecutara un troyano. El troyano en este caso es un software malicioso que se instala en la computadora del usuario que previamente fue identificado como el objetivo para abrir una puerta en secreto, y que autorización, instaló un programa que permitió el acceso remoto de un usuario no autorizado para robar la información contenida en su computadora. Al hacer clic en link malicioso se abre directamente una página de Internet Explorer aprovechando alguna de sus vulnerabilidades.

1.8.5. Night Dragon

según Mcafee (2010), el método de infección que usa es por medio spear phishing attacks, el cual se vale de ataques coordinados, encubiertos y ciberataques dirigidos haciendo uso de técnicas de ataque tales como: la ingeniería social, "spearphishing" de explotación de vulnerabilidades en el sistema operativo Windows, directorios activos y las herramientas de administración remota, o RAT's (Remote Administration Tools).

Modo de operación

1. Los servidores web de internet estaban comprometidos a través de inyección de SQL, malware y administración remota.
2. Los servidores web comprometidos se usan como zombis para realizar ataques contra objetivos internos realizando la técnica de pivote mediante una maquina infectada.
3. Luego estos puntos comprometidos realizan ataques por email con la intención de acceder de manera no autorizada a información confidencial, como también a los dispositivos móviles de los trabajadores. Posteriormente usan usuarios de VPN para obtener acceso interno adicional.
4. El ataque utiliza herramientas de ingeniería social con el propósito de robar credenciales o contraseñas, métodos de acceso o autorización para acceder a otros sistemas. Lo anterior permite la instalación de RAT's, y la instalación de malware a medida que progresa el ataque. Este usa vulnerabilidades similares a las que uso operación AURORA para lograr su cometido.
5. Sistemas pertenecientes a los ejecutivos son objeto de correos electrónicos y archivos que son capturados por los atacantes.

Introducción

1.8.6. Operación Ghostnet

Utiliza la técnica de spear phishing attacks (adjuntos infectados en los correos o enlaces maliciosos en los mismos), similar a **Operación Shady RAT**, Según Holguín, Moreno y

Merino (2013). Cuyo vector de infección es Spear Phishing Attacks (documentos adjuntos Office y PDF infectados).

La intrusión se inicia con un correo dirigido (Spear-Phishing Attack) que incluía un exploit, que era enviado a un usuario con responsabilidades de administración en la organización. Cuando era abierto en un sistema no actualizado, infecta el equipo y descargaba el malware de la fase de intrusión. Este malware instala una puerta trasera que permitía la comunicación con el de Command and Control a través de tráfico HTTP. Esto era aprovechado rápidamente por los atacantes para introducirse por la red interna, realizar escalada de privilegios y afianzar la intrusión dentro de la organización, asegurando la persistencia en la misma. Finalmente, los atacantes extraían información de todo tipo hacia los servidores de control. Symantec (2012) definió tres fases principales. En la primera fase, el vector de infección inicial es por medio de correos dirigidos con ficheros maliciosos anexos de tipo Microsoft Office (ficheros Word, Excel o PowerPoint) y PDF.

Partes de los ficheros analizados aprovechan vulnerabilidades antiguas, como la del programa Microsoft Excel 'Microsoft Excel 'FEATHEADER' Record Remote Code Execution Vulnerability', que se vale de un error en el tratamiento de la cabecera FEATHEADER, con código CVE-2009-3129. El exploit en este caso ejecuta código para descargar un troyano que inicia la segunda fase de la intrusión, conectándose a un sitio remoto para descargar imágenes y ficheros de código HTML, debido a que habitualmente los elementos de seguridad perimetrales de las organizaciones no realizan una inspección exhaustiva.

En este caso se usaron técnicas de esteganografía donde escondían los comandos que serían interpretados por el equipo infectado. Así mismo en los ficheros de código HTML, los comandos venían ocultos en código HTML con comentarios. Cuando el troyano se conectaba con el sitio remoto se producía una conexión inversa con el equipo infectado, lo que habilita al atacante a ejecutar comandos de manera transparente a la víctima.

Introducción

1.8.7. Oak Ridge National Laboratory

Holguín, Moreno y Merino (2013). Afirman que en este ataque el intruso por medio de envió de correos a usuarios que abrieron un adjunto, permitieron utilizar la vulnerabilidad de Internet Explorer de día cero Microsoft para acceder a la red del laboratorio. La

vulnerabilidad, que se describe como una vulnerabilidad que permite la divulgación de información Mediante Propiedad Control. View State, esto permite la ejecución de código remoto, además permite a un atacante instalar malware en la máquina del usuario si él o ella visitan un sitio web malicioso.

1.8.8. APT1

Consiste en envió de correos electrónicos de phishing con links infectados, los objetivos eran redirigidos a un servidor comprometido donde alojaba código JavaScript. Una vez que se identifica un host de destino, las víctimas descargan un archivo Adobe Flash Player SWF malicioso y un archivo FLV. Esto permite generar una puerta trasera de encargo conocida como shotput, detectada por FireEye (2013) como Backdoor APT CookieCutter , entregado al sistema de la víctima. El taque puede hacerse usando un archivo PDF que contiene otros tipos de archivo dentro de ella, por ejemplo, HTML, JavaScript, SWF, XLSX, EXE, archivos de Microsoft Office o incluso otro archivo PDF

Un atacante puede utilizar esta funcionalidad para poder insertar el archivo malicioso dentro de un archivo benigno.

1.8.9. ACAD/Medre.A56

Su finalidad es el robo de proyectos desarrollados en AutoCAD. El malware tiene por objetivo filtrar proyectos industriales localizados en empresas del Perú y transferirlos a servicios de correo alojados servidores ubicados en China. Actúa bajo la modalidad de envió de correos dirigidos con ficheros adjuntos maliciosos, tener acceso a multitud de organizaciones de forma remota. Como se puede apreciar algunos ataques analizados se enfocaron en ciertas organizaciones, pero ninguno puede descartarse, porque son cambiantes y pueden surgir variantes y apuntar a otros objetivos. Como se muestra en las siguientes figuras donde duqu 2.0, es una variante de Stunexnet, flame, Gaus, miniflame, Esta versión de Duqu es sigiloso y reside en la memoria del ordenador, sin archivos escritos en el disco. Mediante envió de correos con archivos adjuntos (documento de Microsoft Word) puede usar as vulnerabilidad del núcleo previamente desconocido que permite la ejecución de código, cuando se abre el archivo, el código malicioso se ejecuta e instala los binarios principales de

Introducción

Duqu. También permite a los atacantes propagar Duqu a otras computadoras en las zonas seguras y controlarlos a través de un protocolo de C & C-peer-to-peer, sin necesidad de que estén conectadas a internet.

Se presenta en dos variantes, la primera es una puerta trasera básica que parece utilizarse para hacerse un hueco persistente dentro de la entidad dirigida por infección de varios equipos y la segunda variante es más compleja, contiene varios módulos que proporcionan una gama de funcionalidad para el malware, tales como la recopilación de información en la computadora infectada, recogida de datos, la detección de redes, infección de la red, y la comunicación con-mando y control (C & C) servidores (Symantec, 2015).

Esquemas de Infección de un ataque APT

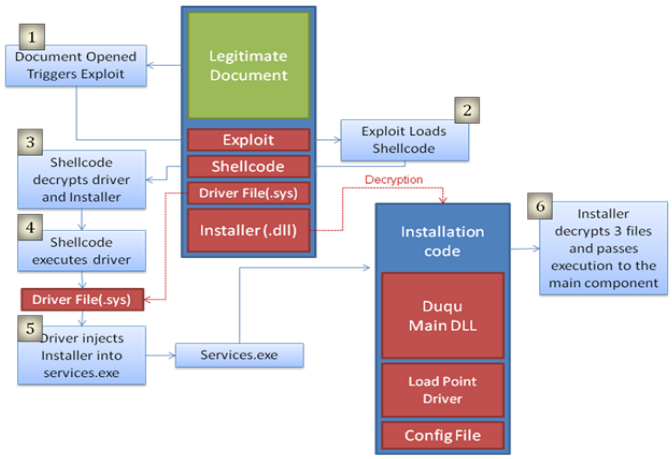


Ilustración 1.Esquema de Infección de un APT

Fuente: symantec

1.9. APT que han atacado el sector salud

1.9.1. Orangeworm.

Esta amenaza infecto grandes organizaciones internacionales de salud en los Estados Unidos, Europa y Asia. La cual se conoce como "kwampirs", el malware explota vulnerabilidades en los dispositivos médicos, entre los que se destacan los dispositivos de imágenes de alta tecnología, como rayos X, Resonancia Magnética Nuclear (RMN), recursos compartidos en red, servidores y software médico donde reposa información de pacientes. También se enfoca en cadena de suministro de materias y equipos médicos, compañías farmacéuticas y los proveedores de soluciones de TI para equipos médicos y de salud (Symantec, 2018).

Introducción

Su modo de infección se basa en infiltrarse en la red de la víctima, mediante la descarga y ejecución de un troyano de puerta trasera llamado kwampirs, que proporciona a los atacantes el acceso remoto a la computadora comprometida. Posteriormente recopila información básica sobre equipos comprometidos y la envía a los atacantes a un servidor remoto de

comando y control. Si la víctima es de su interés, el malware se propaga a través de recursos compartidos de red abiertos para infectar a otros dispositivos del sector salud.

Kwampirs descifra y extrae una copia de la carga útil principal DLL desde su ubicación, pero antes de escribir en disco la carga útil, inyecta una cadena en la carga descifrada de forma aleatoria para evadir las detecciones basadas en hash.

El malware mantiene persistencia manteniendo un servicio y garantiza que la carga se mantenga en la memoria al reiniciar el sistema, a continuación se muestra configuración.

Service name	WmiApSrvEx
Display name	WMI Performance Adapter Extension
Start type	SERVICE_AUTO_START
Binary pathname	%Windows%\System32\<filename.dll>
Command	rundll32.exe "%Windows%\System32\<filename>",ControlTrace -Embedding -k

Tabla 2.Configuración de la carga útil

Fuente: Symantec

Puede copiarse en recursos compartidos de archivos ocultos como en: ADMIN $, C $ WINDOWS, D $ WINDOWS y E $ WINDOWS.

Aunque el método se considera antiguo, todavía es viable para plataformas que ejecutan sistemas operativos antiguos como Windows XP, Windows 7 y 8, pero ha demostrado ser efectivo dentro del sector salud, que puede ejecutar sistemas heredados en plataformas más antiguas diseñadas para la comunidad médica (Symantec, 2018) .

1.9.2. MEDJACK.

Es una APT que infecto una variedad de dispositivos médicos que incluyen equipos de rayos X, sistemas de archivo y comunicaciones de imágenes (PACS) y analizadores de gases en sangre (BGA). Esto incluye equipos de diagnóstico (escáneres PET, escáneres CT, MRI, etc.), equipos terapéuticos (bombas de infusión, láseres médicos y máquinas quirúrgicas LASIK) y equipos de soporte vital (máquinas cardiopulmonares, ventiladores médicos, máquinas de oxigenación por membrana extracorpórea y máquinas de diálisis) entre otros.

Introducción

Así mismo Ríos (2015), Menciona que los modelos de bombas de infusión de medicamentos vulnerables son: las PCA LifeCare, PCA3, PCA5, Symbiq y el modelo de bombas Plum A +, también menciona que hay "al menos 325,000" bombas de infusión de drogas Plum A + actualmente instaladas en hospitales de todo el mundo.

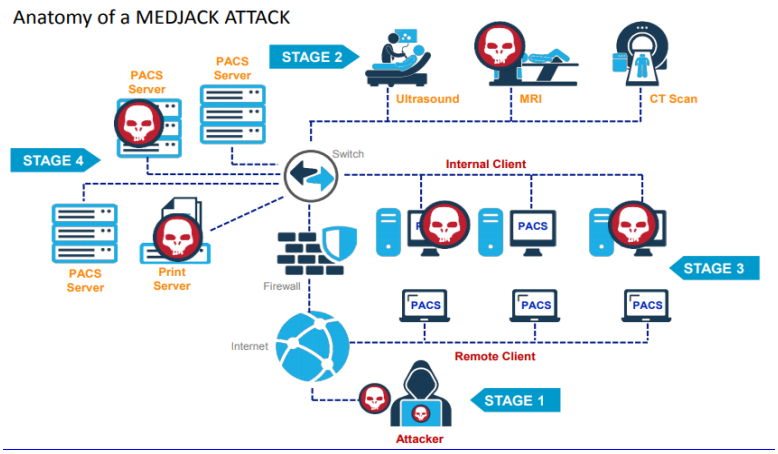


Ilustración 2. Ataque APT medjack

Fuente: TrapX Lab

1.10. Análisis del ciclo de vida de APT teniendo en cuenta el modelo kill chain.

A continuación, en la figura 4, se muestra el Modelo Kill Chain, el cual consta de 7 fases, posteriormente se explica cada una de las fases propuestas.

Modelo del Ciclo de vida del APT, según Kill Chain

Introducción

Ilustración 3. Ciclo de vida amenazas persistentes avanzadas, del modelo seleccionado Kill Chain.

Fuente de elaboración propia

1.10.1. Fase de Reconocimiento

En esta fase se realiza una recopilación de información de los objetivos que se desea infiltrar identificando los puntos débiles de la organización y/o de los empleados. El reconocimiento se puede desglosar identificando los objetivos, luego mirando e identificando los perfiles de usuarios en la organización (Bhatt & Yano, 2013)(Marchetti et al., 2016)**.** También, se valen de las relaciones con otras entidades en donde se pueden apoyar los atacantes para alcanzar el objetivo. Analizan la red para buscar servicios abiertos o desprotegidos, identifican los sistemas de defensa que la organización utiliza, y analizan que empleados tienen acceso a la información específica que les sirva para lograr su cometido, utilizando información de las redes sociales públicas de la que los empleados pueden ser miembros (por ejemplo, LinkedIn, Facebook, etc.).(Giura & Wang, 2013).

El reconocimiento es una de las fases en la que el atacante se toma el tiempo necesario para poder infiltrar el sistema y así poder lograr su objetivo. Para poder realizar dicha intrusión en el sistema el cibercriminal busca fuentes de información (correos corporativos, sitios más visitados, reconocimiento de puertos, sistemas operativos, aplicaciones, entre otros) que sirva como estrategia para lanzar sus ataques dirigidos (Bhatt & Yano, 2013)(Marchetti et al., 2016)**.** Es un paso importante de preparación antes del ataque. Los atacantes identifican y estudian la organización, recopilan toda la información posible sobre el entorno técnico y personal clave de la organización (P. Chen, Desmet, & Huygens, 2014). Para luego en la fase de preparación usar la información vulnerable de la organización y preparar la operación de ataque.

1.10.2. Fase de Preparación de la operación.

Los atacantes en esta fase preparan el entorno a atacar, haciendo uso de malware, el cual diseñan y desarrollan para explorar vulnerabilidades identificadas en la fase 1. El código malicioso se desarrolla de tal forma que tiene la capacidad de acoplarse a formatos insospechadas como pdf, doc y ppt (P. Chen et al., 2014)(Bhatt et al., 2014). También, ponen

Introducción

en marcha servicios maliciosos, para engañar a los usuarios a que hagan uso de estos (Luh et al., 2017). La preparación puede consistir en un correo electrónico de phishing dirigido, utilizando información que reunieron en la etapa de reconocimiento.

En este caso, el correo electrónico de phishing, podría contener una invitación a un evento, rifa, ofertas, pago de servicios, que son programados por una organización en el que el empleado objetivo confíe y proceda a realizar un clic sobre la URL y descargar un archivo con documentos o archivos adjuntos infectados. En la gran mayoría de los casos el correo electrónico es el vector de infección, más usado en la fase de distribución para entregar el malware, pero también se pueden usar otros canales, tales como medios extraíbles USB y sitios Web de baja reputación (Giura & Wang, 2013).

1.10.3. Fase de Distribución

En ésta fase los atacantes tienen conocimiento fuerte de su objetivo y de los empleados, que se identificaron en la fase 1. La organización criminal tiene todo lo que necesitan para empezar a buscar un punto de ingreso a la red de la compañía y establecer uno o varios accesos permanentes. Generalmente los atacantes se aprovechan de vulnerabilidades que la víctima no ha identificado (William F. Crowe, CISA, CISM , CRISC, 2015), (P. Chen et al., 2014), (Bhatt et al., 2014). En esta fase para realizar la entrega, el atacante utiliza varios canales de entrega, ya sea correos, sitios web, medios extraíbles USB, etc. (Luh et al., 2017), para engañar a los usuarios de la organización, usando tácticas de engaño, mencionadas en la fase 2.

1.10.4. Fase de explotación

Esta fase se centra en la entrega de carga útil a la víctima anfitrión, la explotación desencadena código malicioso para realizar la intrusión (Luh et al., 2017). La explotación se dirige a una vulnerabilidad de software de aplicación o software operativo y aprovecha una característica del sistema operativo que permite auto ejecutar el malware o código malicioso (Yadav & Rao, 2015). Esta es la fase más crítica, ya que mediante vulnerabilidades existentes en el software permite acceder al sistema y tener control total de este. La vulnerabilidad es el error de software que puede resultar en una amenaza potencial para el sistema. Un error de software es una condición inesperada en la que el software se porta mal (Medina, 2014). Una vez el malware ingrese en la red de la organización por medio del empleado seleccionado, el malware descargado por engaño, se instala y se activa. Para más tarde crear una conexión de

Introducción

comando y control (C & C), desde la máquina víctima hasta la computadora del atacante. Una vez asegurada la conexión de C & C, los ciberdelincuentes continúan en silencio recopilando información sobre las configuraciones de seguridad de la computadora infectada y de los equipos conectados en red, también recopila información del sistema relacionada,

las contraseñas, recopilan mensajes de correo electrónico de usuario para soportar futuros ataques (Giura & Wang, 2013).

1.10.5. Fase de Instalación

Después de lograr explotar una vulnerabilidad en la fase anterior, el atacante puede acceder al sistema de la víctima y lograr la persistencia en la máquina infectada y así tener acceso a la información objetivo de su ataque, mediante el uso de programas que permiten instalar el malware, tales como:

Dropper: Diseñado para instalar malware (virus, backdoors, otros) a un sistema de destino y evitar ser detectados por los programas antivirus. Una vez activado dropper puede ser utilizado para robar la identidad o para dañar el rendimiento de los equipos (Yadav & Rao, 2015).

Downloader: Programa que permite descargar automáticamente caratulas de música con código maligno y posteriormente instalar el malware y ocultarlo para evitar ser detectado por el sistema antivirus (Yadav & Rao, 2015).

En esta fase se valen de las vulnerabilidades explotadas para realizar inyección de código, dejar gusanos o troyanos, buscar otros kits de Exploits y realizar suplantación de identidades o realizar fraude. Dicha fase en la que la carga útil entregada aprovecha una vulnerabilidad y se instala en la máquina de la víctima (Crowe, 2015). También, se considera la fase donde los atacantes usan técnicas de instalación de malware en secreto, para explotar las vulnerabilidades a nivel de sistema operativo, de software aplicativo y a nivel de red, para hacerse con los sistemas, causando denegación de servicios, ejecución de código remoto o local, escalar privilegios, deficiencia en el proceso de negociación en el protocolo TLS, SSL, corrupción de memoria, error de entradas invalidas, buffer overflow, dangling pointer, use after free y bypass.

Introducción

1.10.6. Fase comando y control.

Esta fase el atacante obtiene el comando y control de la máquina infectada, denominado C&C, después de haber explotado una vulnerabilidad del sistema, mediante el uso de troyanos, botnets y denegación de servicios. El sistema de comando y control es usado para

dar instrucciones remotamente a una maquina comprometida (Yadav & Rao, 2015). El comando y control se puede obtener usando estructuras de comunicación.

Entre ellas se destacan, tres tipos de estructuras de comunicación de comando y control, la estructura tradicional centralizada, la peer-to-peer (método para intercambio de archivos, programas, aplicaciones, vídeos o fotos) descentralizada y las más recientes redes sociales basadas en última estructura. En este caso la carga útil se instala y establece la conexión saliente con el entorno del atacante para permitir la interacción con el adversario malintencionado (Crowe, 2015). Hay que tener en cuenta que los atacantes se valen de canales anónimos de comunicación de malware como IRC Chats, TCP, HTTP, FTP, Esteganografía, TOR, DNS Fast Flux, DNS como medio y algoritmos de generación de dominios para sustraer información sin ser detectados.

1.10.7. Fase De Acciones Sobre Objetivos.

Después de lograr configurar la comunicación con el sistema de destino, el atacante ejecuta los comandos necesarios de acuerdo a los intereses que dieron inicio al plan de ataque (Yadav & Rao, 2015). Esta es la fase final de un ataque APT, donde el atacante está en posición para hacerse con los datos objetivos. Dependiendo del tipo de objetivo, esta actividad puede incluir robo de información de cuentas bancarias, correos electrónicos, redes sociales, credenciales de administrador y manipulación de información confidencial o secreta, extracción de datos, etc. (Crowe, 2015)

Introducción

1.11. Herramientas de prevención y mitigación

Son aquellas que un atacante puede eludir ante una medida preventiva a la hora de atacar una organización. Su objetivo es minimizar el daño o prevenirlo lo antes posible. Debido a que

la detección se produce durante un ataque en ciertos casos, y donde el tiempo de reacción es crítico (Cole, 2013).

La respuesta: Se ocupa del daño después de que se detecta y uno de sus objetivos es solucionar el problema, asegurarse de que no vuelva a ocurrir y recuperar la organización (Cole, 2013). Vale la pena destacar que la detección implica que una medida preventiva falló. Es decir se debería prevenir todos los ataques, esto significa que si se detecta un ataque, significa que la prevención no fue efectiva y se debe de buscar formas de hacerlo efectivo (Cole, 2013)

Hay que recordar que los APT son ataque sigilosos, la prevención es ideal y la detección es una necesidad y la única posibilidad de contener un daño. Dado que la detección se produce durante un ataque, esto significa que hay algún daño en su organización y seguridad no fue efectiva como debería frente a este tipo de amenazas poniendo en riesgo los datos e información sensible de la entidad hospitalaria (Cole, 2013).

1.12. Modelo Kill Chain

El modelo Kill Chain patentado por Lockeheed Martin, es uno de los modelos más aceptados al momento de detectar cualquier tipo de amenaza, ya sea una amenaza tradicional o una amenaza persistente avanzada, el cual permite aplicar estrategias proactivas de prevención y detección temprana para dar respuesta, contención y mitigación a los incidentes APT. Dicho modelo fue eligido para el desarrollo de la tesis, teniendo en cuenta lo anteriomente mencionado y por la trayectoria del autor Lockeheed Martin en seguridad informática, el cual ha sido citado en más de 235 artículos como se muestra en la tabla 23, donde se lista según los autores que proponen el modelo Lockeheed Martin.

1.13. Pruebas de penetración.

Son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar, buscan medir la confidencialidad, integridad y disponibilidad de la informaicon; se parte de identificar los riesgos y amenazas desde el uso del usuario final, suelen también utilizarse para probar el cumplimiento de la

Introducción

política de seguridad de una organización, la conciencia de seguridad de sus empleados y la capacidad de la organización para identificar y responder a los incidentes de seguridad.(Margaret, 2015)

Existen varios tipos de pruebas las automatizadas con aplicaciones de software y las manuales, ambas buscan determinar las debilidades de seguridad. (Margaret, 2015)

ISSAF como un framework de evaluación de Seguridad de Sistemas de Información. Su meta principal es proporcionar procedimientos muy detallados para el testing de sistemas de información que reflejan situaciones reales, se utiliza para cumplir con los requisitos de evaluación de las organizaciones y puede utilizarse además como referencia para nuevas implementaciones relacionadas con la seguridad de la información. Incluye los siguientes ítems: Descripción de criterios de evaluación, Finalidades, objetivos, prerrequisitos para la realización de las evaluaciones, procesos para las evaluaciones, presentación de resultados, contramedidas recomendadas y referencias a documentos externos, este framework propone cinco fases: Fase I – Planeación, Fase II – Evaluación, Fase III – Tratamiento, Fase IV – Acreditación, Fase V –Mantenimiento (Prandini & Ramilli, 2010).

OSSTMM como la recopilación de metodologías para pruebas y análisis de seguridad realizado siguiendo la metodología OML (Open Methodology License) es de libre uso y distribución, como también se pueden realizar las siguientes pruebas: Humanos, físicos, wireless, telecomunicaciones, y redes de datos. Al tiempo que se centra en los detalles técnicos básicamente en lo que debe de someterse a la prueba, qué hacer antes, durante y después de una prueba de seguridad, y cómo medir los resultados.

PTES, son pruebas estándar de ejecución consta de siete (7) secciones principales, el cual proporciona todo lo que tiene que ver con una prueba de penetración, cubriendo desde la primera comunicación y el razonamiento detrás de un pentest, hasta la presentación de informes, que captura todo el proceso, de manera que tenga sentido para el cliente y proporciona mayor valor (Wang et al., 2013).

Introducción

2.Metodología

La metodología que se propuso para dar respuesta a los objetivos de esta tesis se basarón en investigación, observación, descripción de proceso técnico y documental. En donde se estructuró en cuatro fases, donde en cada una resume las actividades que se realizarón para lograrlos.

2.1. Identificación y definición de los activos del sector hospitalario.

Se propuso una guía para la identificación de activos sensibles a fuga de información, esta guía fue el resultado de una revisión sistemática de diferentes normas y estándares nacionales, guías de buenas prácticas enfocadas a la identificación de activos. Esta cuenta con fases flexibles y obligatorias que permiten a la entidad hospitalaria, seleccionar la fase que se adecue a sus necesidades. La guía cuenta con un artefacto en Excel, (Ver anexo A Item 6.1 Artefacto para realizar levantamiento de Activos del sector Hospitalario que se propone en la guía.) para el registro, valoración de los activos y modelado de amenazas (Ver tabla 61 del anexo A "Artefacto para realizar levantamiento de Activos del sector Hospitalario que se propone en la guía".) que permiten identificar los requerimientos del framework, que facilitan a la entidad hospitalaria a identificar los activos sensibles a fuga de información por correo electrónico.

Para la cual se realizó una búsqueda en diferentes portales y documentos tales como el ministerio de salud en su portal www.minsalud.gov.co, de los cuales se tomo algunos ítem de referencia para la clasificación de los activos de información. Además se toma como referencia la ley 1712, en la cual estipula en al artículo 13, la forma que deben realizar registros de activos de información. "Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo uso de: a) Todas las categorías de información publicada por el sujeto obligado, b) Todo registro publicado. Todo sujeto obligado deberá asegurarse de que sus Registros de Activos de información." (Congreso Nacional de la República de Colombia, 2014). Asi mismo se tomo como referencia las guias que proponen en el portal de la Supersalud https://www.supersalud.gov.co, dichas guias contienen una serie de instrucciones tales como: información de línea base para la gestión de

Introducción

activos, formatos de instrumento de gestión de la información, gestión de incidentes, gobierno y gestión de la información, guía de gestión de activos, seguridad en las operaciones, que le permitirán a las entidades de salud, conocer los estándares mínimos para

tener una buena gestión de los activos y de la información que reposa en ellos como también la información que estos gestionan.

Por ultimo la guía que surge en esta tesis es el resultado también de la compilación de estrategias del MINTIC, donde reposan elementos para promover buenas prácticas. En este caso se tomaron elementos del portal http://www.mintic.gov.co/gestionti/615/w3-article-5482.html , la cual es una estrategia del gobierno que está promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

Estas son fácilmente adaptables a cualquier empresa del estado. Para ello cuenta con varias guías: a. **Política General**, establece que para la gestión de activos se debe contar con: la identificación del activo, clasificación, etiquetado de la información, devolución de activos, Gestión de medios removibles (Ministerio de las TIC, 2016a), b. **procedimiento de seguridad**, establece que para la gestión de los activos de información; que son identificados por la entidad, deben de clasificarse de acuerdo a su nivel de confidencialidad o criticidad como también un procedimiento que esta debe de seguir cuando el activo ya no se requiera (MINTIC, 2016f), c**. Guía para la Gestión y Clasificación de Activos de Información**, establece que para la identificación del inventario de activos de información, es importante puesto que permite determinar a cual se le debe brindar mayor protección, permitiendo identificar claramente sus características y rol al interior de un proceso (MINTIC, 2016d).

Todos estos trabajos a pesar de hacer parte de portales del ministerio de salud y del ministerio de las TIC, no especifican un procedimiento sistemático y secuencial para identificar activos sensibles a la fuga de información en el sector salud, puesto que son un conjunto de buenas prácticas que cualquier empresa debe adoptar para asegurar sus procesos frente algún tipo de amenaza, pero a nivel muy general. La guía que se propone no aisla las otras guias y estandares, mas bien es el resultado de la compilación de todas las anteiores y se enfoca al sector salud permitiendo la identificación de los activos sensibles a la fuga de información, de manera que se pueda promover un tratamiento de los riesgos.

Introducción

2.1.1. Identificación de los diferentes tipos de APT que causan fuga de información y definición de una lista de chequeo donde se refleje el tipo de APT a cuál tipo de activo se dirige y priorización de los activos más propensos a la fuga de información por APT.

Se realizó una búsqueda sistemática en diferentes bases de datos bibliográficas y publicaciones que incluyen proveedores y proyectos, investigadores de vulnerabilidad, CERT nacionales y de la industria y programas de recompensas de errores, donde se hizo un énfasis en ataques recientes de amenazas persistentes avanzadas que han ocasionado fuga de informacion y que hallan usado el correo electrónico como medio de propagacion, esto por que el correo electrónico en el sector salud es usado para la gestión de información y lo han convertido en un blanco muy apetecido por los cibercriminales, para lanzar ataques dirigidos a empleados usando el correo electrónico. (Ver ítem 3.1.17, tabla 23 "Clasificación de los nivel de fuga de información")

Tambie se realizó una busqueda de los ataques mas comunes y se determinó cuales ataques apuntaban a cierto perfil de empleados y se hizo una descripción del funcionamiento y afectación de las campañas de APT que utilizan con frecuencia tácticas de spear-phishing, como también se identificó y clasífico las vulnerabilidades que explotan dichas APT y los sistemas que afecta, teniendo en cuenta su nivel de impacto teneindo en cuenta recomendaciones de investigadores de vulnerabilidad.

2.1.2. Identificacion del funcionamiento de un APT proveniente de correo electrónico, su operación en cada fase e identificación de la fase mas sensible a fuga.

Para esta actividad se hizo una compilación e investigación de diferentes bases de datos bibliográficas en las cuales se han mostrado los diferentes tipos de ataques que se han presentado y su forma de penetración, técnicas y tiempo de duración en sistemas sin ser detectadas. De las cuales se realizó un análisis técnico de generacion e implantación de malware que usan la mayoría de APT (Ver anexo E, ítem 6.5. Análisis técnico), Entre los multiples estudios se han presentado diversas fases según los estudios, entre los que se destacan los siguientes: "modelo de concientización en la prevención de la fuga de información", "cyber attack modeling analysis techniques: an overview", "the modern day attacker", advanced analytics a proactive approach to cybersecurity, entre otros. De los cuales se identificaron varios modelos que definen las fases del ciclo de vida de las APT, los cuales van dirigidos a activos de la organización. Entre ellos están el modelo Kill Chain que consta

Introducción

de 7 fases (Yadav & Rao, 2015), el cual se seleccionó para la investigación, debido a que se usará para describir las fases por las que atraviesa una campaña APT y en cada fase permite detectar amenazas y prevenirlas de forma proactiva. Por otro lado, los modelos como: LogRhythm considera un modelo que consta de 5 fases APT (Id Messaoud et al., 2016), el

modelo de Lancaster tiene en cuenta 3 fases, el modelo SDAPT, al igual que el modelo de BSI constan de 8 fases (Drinkwater, 2014). En todos los modelos presentados anteriormente, las fases representan las acciones de los atacantes, esto significa que solo se basan en los movimientos de los atacantes para identificar ataques. Al centrarse en las acciones de los atacantes, puede conllevar a acciones erróneas. Además, existen cientos de mecanismos de ataques para hacerse con los objetivos, como los menciona el estándar de clasificación de patrones comunes de ataque (CAPEC) (CAPEC, 2017). En algunas situaciones, los atacantes por lo general usan acciones desconocidas, que no están listadas en modelos anteriores y que tiene sus propios mecanismos para identificar su objetivo, por tanto, es importante centrarse en identificar las buenas prácticas en cada una de las fases del APT, teniendo en cuenta los ataques más usados usando técnicas de ingeniería social.

A continuación se presenta la Tabla 3 donde se realiza un resumen de las fases del ciclo de vida APT de acuerdo a diferentes modelos propuestos por los autores (Id Messaoud et al., 2016.), (Drinkwater, 2014), (R. Lee, Assante, & Conway, 2014), (Assante & Lee, 2015), (INCIBE, 2016), (Bhatt, Yano, & Gustavsson, 2014).

Permite	• Identificar Amenazas dirigidas contra un objetivo. • Reconocer las acciones y eventos de los atacantes. • Mitigación de la amenaza	Reconocer las acciones y eventos de los atacantes.			
Fases/Modelo	Kill Chain	Modelo LogRhythm	Modelo Lancaster	Modelo SDAPT	Modelo BSI
1	Reconocimiento	Reconocimiento	Reconocimiento, inicio de Ataque, infección inicial de host	Reconocimiento	Observar la victima
2	Militarización	Compromiso	Intrusión de red, Control remoto, Movimiento lateral, descubriendo datos, persistencia	Ganando acceso	Preparando ataque distractor
3	Entrega	Manteninedo el acceso	Puesta en escena del servidor seleccionado, preparacion de datos y extracción de datos	Reconocimiento interno	Primera infección
4	Explotación	Movimento lateral		Ampliar acceso	Observar la red
5	Instalación	Extracción de datos		Reuniendo información	Obtener mas derechos
6	Mando y Control			Extracción de información	Espionaje de datos, sabotaje del sistema
7	Acciones sobre Objetivos			Control de fugas de información	Observación continua
8				Borrado de huellas	Borrado de pistas

Tabla 3 Resumen de las fases del ciclo de vida APT

Fuente: Adaptado http://www.itrans24.com/

Introducción

Como vemos a partir de la tabla anterior son varias las fases del ciclo de vida, de acuerdo a los modelos propuestos por varios autores se observan que los modelo propuesto por Kill Chain y el modelo propuesto SDAPT y el Modelo BSI son los modelos que más fases proponen para el ciclo de vida de las amenazas persistentes avanzadas.

Se hizo una selección del modelo de Kill Chain por ser un modelo que identifica las amenazas avanzadas persistentes avanzadas, reconoce las acciones y eventos de los atacantes al igual por ser un modelo que dispone de estrategias de mitigación de dicha amenaza. Para justificar de forma más precisa este modelo se comienza a realizar la revisión de la literatura de 2013 hasta 2017 para mirar cuál es el modelo más citado y usado por los autores, como también se hizo una búsqueda de cuantas veces fue citado el autor en artículos relacionados con el modelo. A continuación, se muestra la tabla 4 con autor y artículo que mencionan el modelo seleccionado.

Resumen de artículos que resumen modelo Kill Chain

Artículo que lo menciona	**Fuente**	**Autor**	**Citado**
1. Ciber amenazas emergentes: a que nos enfrentamos	Revista	Víctor acin sanz ramon vicens lilo	No
2. Advanced analytics a proactive approach to cyber 3. Security	Tesis	Anthony d. Ombrellaro, jr	No
4. Improving security using deception	Tesis	Hammed h. Almeshekah, eugene h. Spafford and mikhail j. Atallah	7
5. Cyber threat indications & warning: predict, identify and counter	Articulo revista	scott swanson, craig astrich and michael robinson	2
6. Expanding the cyber kill chain for embedded system architectures	Tesis	Val a. Red	No
7. Active cyber defense a framework for policymakers	Artículo de revista	Irving lachow	No
8. Proposed cybersecurity t&e process	Articulo mitre	Mr pete christensen	1
9. Cyber-attack thread: a control-flow based approach to deconstruct and mitigate cyber threats	Articulo IEEE	Koustav sadhukhan∗ , rao arvind mallari.	No
10. Moving Target Network Defense Effectiveness Evaluation Based on Change-Point Detection	Research articulo	Cheng Lei,1,2 Duo-he Ma,3 Hong-qi Zhang,1,2 and Li-ming Wang3	4

Introducción

11. Countering Advanced Persistent Threats through Security Intelligence and Big Data Analytics	Articulo IEEE	Fabio Pierazzi, Mirco Marchetti, Alessandro Guido, Michele Colajanni	0
12. Lateral Movement Detection Using Distributed Data Fusion	Articulo IEEE	Ahmed Fawaz∗ , Atul Bohara† , Carmen Cheh† , William H. Sanders∗	0

13. Advanced persistent threat: new analysis driven by life cycle phases and their challenges	Articulo IEEE	Brahim i d messaoud ; karim guennoun; mohamed wahbi ; mohamed sadik	No
14. Early Detection of Cyber Security Threats using Structured Behavior Modeling	ACM	Xiaohua Yan, Carnegie Mellon University Joy Ying Zhang, Carnegie Mellon University	1
15. Advanced persistent threats: behind the scenes	Articulo IEEE	Martin ussath ; david jaeger ; feng cheng ; christoph meinel	2
16. Terminaptor: highlighting advanced persistent threats through information flow tracking	Articulo IEEE		0
17. A study on Advanced Persistent Threats	Articulo IEEE	Ping Chen, Lieven Desmet, and Christophe Huygens	33
18. Defendable Architectures Achieving Cyber Security by Designing for Intelligence Driven Defense®	Articulo Página oficial Martin Lochie	Scott C. Fitch, Michael Muckin Lockheed Martin Corporation	0
19. Analyzing Targeted Attacks using Hadoop applied 20. to Forensic Investigation	Articulo IEEE	Parth Bhatt1, Edgar Toshiro Yano	3
21. Detection of APT Malware through External and Internal Network Trac Correlation	Tesis de maestría	Terence Slot	2
22. A Markov Multi-Phase Transferable Belief Model: An Application for predicting Data Exfiltration APTs	Articulo IEEE	Georgios Ioannou Panos Louvieris Natalie Clewley Gavin Powell	8
23. Towards a Collaborative Framework to Improve Urban Grid Resilience	Articulo IEEE	O Jung, S Bessler, A Ceccarelli, T Zopp	3
24. Technical Aspects of Cyber Kill Chain	Articulo simposio	T Yadav, AM Rao	2
25. Mitigating malicious insider cyber threat	Tesis de maestria	Jason Anthony Smith	2
26. Towards a framework to detect multi-stage advanced persistent threats attacks	Articulo IEEE	Parth Bhatt1 , Edgar Toshiro Yan	25
27. Intelligence-driven computer network defense informed by analysis of advesary campagin and intrusion kill chain	Articulo	Eric m. Hutchins∗ , michael j. Cloppert† , rohan m. Amin, ph.d Lockedh martin	230

Tabla 4 Muestra el número de veces que fueron citados los autores tomados como referentes en la investigación

Fuente de elaboración propia

Los autores hacen referencia al modelo de Kill Chain; en donde muchos de estos explican de forma clara y exhaustiva como los atacantes deben de progresar completamente a través de todas las fases para poder lograr su cometido, dependiendo de los intereses que desea el

Introducción

atacante, aprovechándose de algunas vulnerabilidades presentes en los sistemas. Además, se encontró que este modelo, es el más citado y usado por los autores dedicados al estudio de las amenazas persistentes y al ciclo de vida que estás usan. Se dará una descripción de cada

fase del Modelo de Kill Chain (ver Ilustración 3 Ciclo de vida amenazas persistentes avanzadas del modelo Kill Chain), patentado por Lockeheed Martin.

2.2. Definición de políticas y buenas prácticas que permitan mitigar la fuga de información en los activos sensibles del sector hospitalario, en cada una de las fases del ciclo de vida del APT.

En el objetivo 2, se propuso un conjunto de buenas prácticas y herramientas tanto técnicas como humanas (Ver anexo B, ítem 6.2 Buenas prácticas y políticas). Para la construcción de buenas prácticas y políticas se hizo una evalución a partir de la revisión de varios estándares tales como ITIL, COBIT, HIPPA, ISO 27000, NIST 800-53, ISO 20000 e ISO 27799, realizandose una adaptación a las necesidades del sector salud las cuales han avanzado de manera considerable en el uso de procesos informáticos. Para la construcción de las buenas practicas y de las políticas se busco que los estandares cumplan con:

- Mantener un entorno físico seguro que permite la adopción de tecnologías adecuadas para evitar la fuga de datos al igual que permita la protección de datos y cumplir con la continuidad. (A. H. C. Chen, Chu, & Wu, 2012).
- Evaluacion de los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.(Ministerio de las TIC, 2016b)
- Tener un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios. (Ministerio de las TIC, 2016b)
- Contener políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente, al igual con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos . (Ministerio de las TIC, 2016a).

Se establecieron los siguientes criterios de búsqueda en los estandares:

1. Control de acceso y privilegios de usuario

Introducción

2. Clasificaciónde activos según su criticidad
3. Buenas prácticas para la seguridad de la información
4. Controles de seguridad de la información
5. Atención de incidentes y eventos de seguridad de la información

6. Control para fuga de información
7. Continuidad del negocio
8. Orientación al sector salud

Luego se comenzó a compilar estándares y determinar cuales cumplian uno o mas criterios; como se evidencia en la tabla 5:

Normas y Estándares internacionales

Framework	Control de acceso y privilegios de usuario	Clasificación de activos según su criticidad	Buenas prácticas para la seguridad de la información	Controles de seguridad de la información	Atención de incidentes y eventos de seguridad de la información	Control para fuga de información	Continuidad del negocio	Orientación al sector salud
ITIL			X		X		X	
COBIT	X		X	X	X	X	X	
HIPPA	X	X	X	X	X	X		X
ISO 27000		X	X	X				
NIST 800-53	X	X	X	X	X			
ISO 20000				X	X		X	
ISO 27799			X	X		X		X

Tabla 5. Estándares tomados como referencia

Fuente de Elaboración Propia

2.2.1. Proponer buenas prácticas para mitigar la fuga de información ocasionada por APT, en el sector hospitalario Colombia

A partir de los estándares que se indican en la tabla 5, se procedio a mapear los controles de los diferentes estándares que permitieran establecer los controles de seguridad de la información que apunten a mitigar la fuga de información ocasionada por APT proveniente de correo electrónico; cada grupo de controles fueron construidos con base en áreas (procesos) (salvaguardas Administrativas, Físicas y Técnicas) y responden a intereses y

Introducción

necesidades organizacionales basadas en la visión de la entidad hospitalaria, como lo dice HIPPA (HHS, 2017).

Los controles están seleccionados a partir de ITIL, COBIT, HIPPA, ISO 27000, NIST 800-53, ISO 20000 e ISO 27799, estos controles van a permitir identificar y proteger contra

amenazas a la seguridad o integridad de la información; también están diseñadas para proteger contra usos o divulgaciones inadmisibles y en términos generales asegurar el cumplimiento por parte de por parte de los empleados.(Ver anexo B Buenas practicas y politicas).

Las salvaguardias Administrativas: Son prácticas diseñadas para controlar las medidas de seguridad y la conducta del personal que accede, se procesa y distribuye electrónicamente información médica protegida. Las salvaguardias Físicas: Son procesos que protegen equipo físico y edificios relacionados, de peligros naturales y medio ambientales, así como de intrusiones físicas. Salvaguardias Técnicas: Son mecanismos técnicos y procesos diseñados para proteger, controlar y monitorear el acceso a la información (HHS, 2017). A continuación se muestran las salvaguardas y que controles apuntan a este.

Cada uno de los controles asociados a los salvaguardas, hacen referencia a lo que debe responder cada uno de los controles. Se busco estándar por estándar y se determinó cual apunta a cada uno de los controles de los salvaguardas.

Se hizo la homologación como se indica en la tabla 6 de cada una de las salvaguardas de los estándares, generando los resúmenes de cada uno de los salvaguadas físicas, administrativas y técnicas y que hacen parte del anexo A.

SALVAGUARDAS FISICAS	Limitación y controles de puertos de red	
	Controles de acceso para wifi	
SALVAGUARDAS TÉCNICAS	Controles Criptográficos	
	Mantenimiento, monitoreo, análisis y auditoria de logs	
	Evaluación, remediación y gestión de vulnerabilidades	
	Seguridad en aplicaciones de Software	
	Líneas base de seguridad	
	Defensa ante Malware	
	Test de penetración	
	Gestión de Activos	Inventario de Hardware

Introducción

SALVAGUARDAS ADMINISTRATIVAS		Inventario de Software
		Inventario de datos e información
		Control de uso y administración de privilegios

	Gestión de identidades, privilegios y accesos	Seguridad y configuración de Hw y SW
		Controles de acceso basados en la necesidad de conocer
	Gestión de incidentes y continuidad del negocio	Evaluación y remediación de la continuidad
		Administración, respuesta y gestión de incidentes
	Compromiso de la alta dirección	

Tabla 6 Salvaguardas Vs Controles

Fuente de elaboración: Adaptacion HIPPA

2.3. Caracterización de herramientas para la ejecución de las buenas prácticas propuestas en el framework.

Se realizó análisis de documentos que tenían rigor científico de autores reconocidos y mas citados y que trabajan el modelo de Kill Chain, donde se identificarón una serie de riesgos (ver anexo C, tabla 74 Resumen de técnicas de prevención y detección según el ciclo vida de las amenazas persistentes avanzadas , ítem 6.3 Pruebas de Herramientas), por cada fase del APT, además se hicieron pruebas para medir la efectividad de las herramientas que ayudan a la gestión de amenazas persistentes avanzadas que se asocian al ciclo de vida según el modelo Kill Chain (Ver Anexo C, ítem 6.3. Pruebas de herramientas). Las cuales permitirán a la entidad hospitalaria reducir el impacto y la probabilidad de este tipo de amenazas en sus infraestructuras, al igual que le permite a la entidad seguir cada una de las fases del ciclo de vida de las amenazas persistentes avanzadas, en caso de ser víctima de este tipo de ataques. Como se menciono anteriormente se realizaró un estudio de varios documentos científicos y técnicos que permitierón identificar, clasificar las herramienta y estrategías que mitiguen dichos riesgos y asociarlos a las amenazas que se identificarán en la guía de activos sensibles a fuga de información que se propone como resultado de la etapa 1. Las herramientas fueron probadas en ambientes virtuales y máquinas físicas teniendo en cuenta el riesgo y la fase del apt donde aplica cada una de ellas. Ver anexo C, ítem 6.3, Pruebas de herramientas(véase también ítem 6.3.1 “Pruebas de filtros web”, 6.3.2. “Prevencion de entrada de malware”, 6.3.3. “Herramientas antivirus”, 6.3.4, “Herramientas firewall”, 6.3.5 “Herramientas de

Introducción

análisis de logs y monitoreo”, 6.3.6, “Herramientas IDS/IPS, simulación de ataques, scaneo, etc., 6.3.7. “Herramientas DLP”).

2.4.Construcción del framework

Para dar cumplimiento a esta etapa, se realizaron las siguientes actividades: Definir las entradas y salidas del framework, artefactos y aplicabilidad del framework involucrados, para lo cual se unifican los resultados obtenidos en objetivo 1, 2 y 3 que sirven como insumo en esta etapa. (Ver anexo A, B, C y D, Anexo A. Artefacto para hacer levantamiento de activos en el sector hospitalario, Anexo B. Buenas Prácticas y políticas, Anexo C. Pruebas de herramientas, Anexo D. Pruebas del framework de seguridad informática.).

Para las actividades anteriormente mencionadas se realizo una búsqueda sistemática de la literatura de normas, estándares nacionales e internacionales, frameworks propuestos por autores, guias de levantamiento de activos de información establecidas por el Mintic, entre otras, también se estudio el modo de operación de las APT y se identifico y clasificó las vulnerabilidades aprovechadas por estas (Ver tabla 22, Lista de Vulnerabilidades aprovechadas por las APT, ítem 3.1.17), clasificación según cve.mitre.org (Ver Anexo A, ítem 6.1. Pruebas del framework de seguridad informática.). Todo lo anterior permitio establecer los principios y lineamientos que sirven como entradas del framework, en este caso para definir la guía de identificación de activos sensibles a fuga de información con sus respectivas amenazas que fueron modeladas después de un estudio riguroso de normas de gestión de riesgos que se complementaban para la construcción de los artefactos necesarios y garantizar la identificación de activos, amenazas y riesgos asociados ver tablas 24 a 31, tambien (Tabla 22. listado de las vulnerabilidades aprovechadas por los apt, tabla 23. Apt vs sistemas afectados, Anexo E.configuración de la carga útil (Análisis técnico), tabla 27. modelos amenazas persistentes avanzadas, tabla 28. Muestra el número de veces que fueron citados los autores tomados como referentes en la investigación, tabla 29. Riesgos fase de reconocimiento, tabla 30. Riesgos fase de militarización, tabla 31. Riesgos fase de distribución)(el cual denominamos entrada 1- 2. Dichos elementos se aprecian en la ilustración 9), de la cual surge un artefacto (software) para realizar dicho proceso como se muestra en la tabla 75 a 77. (Tabla 75. Calculando nivel de fuga de información, tabla 76.activos con considerable nivel de fuga de información,tabla 77.activos con nivel fuga críticos y con posibles amenazas) respectivamente y en el anexo D Anexo D. Pruebas del

Introducción

framework de seguridad informática, el cual se desarrollo bajo un entorno de programación web diseñado en html5, css, php y Mysql.

Posteriormente se procedió a realizar el análisis del ciclo de vida de las APT en los diferentes modelos de ataque como se aprecia en la tabla 3 (Resumen de las fases del ciclo de vida del

APT). Luego se determinó que el modelo que se adapta a nuestro framework es el Modelo Kill Chain que se muestra en la ilustración 3 (Ciclo de vida de las amenazas persistentes avanzadas). Por último se procedió a realizar investigación de publicaciones científicas en guias y estándares nacionales e internacionales, pautas para proteger la confidencialidad y privacidad de la información del paciente y sus datos médicos, que permitieron sacar un conjunto de buenas prácticas, herramientas e identificación de riesgos presentes en cada una de las fases del ciclo de vida del APT seleccionado, de tal forma que el framework se diseño como una guia estratégica cuyo enfoque conceptual se asemeja a un DLP.

2.5 Proponer casos de prueba para validar la aplicabilidad del framework en la mitigación de la fuga de información en el sector hospitalario, ocasionadas por APT proveniente de correo electrónico.

Para realizar esta fase se propusieron las siguientes actividades:

Solicitar a una entidad hospitalaria la lista de activos informáticos y conectados en red.

En esta actividad se hizo el contacto con la entidad hospitalaria de Santander de quilichao, llamada QUILISALUD. Donde ellos suministraron la lista de activos en formatos excell, con un compromiso de confidencialidad por parte de los investigadores. En las entidades de Medellin fue imposible debido a la desconfianza de la parte directiva en entregar este tipo de información. Luego se procedió con las recomendaciones que surgen del objetivo 1 de levantamiento de activos. Donde se identificaron del un total de 99 activos un grupo de estos que eran sensibles a fuga y que fueron clasificados teniendo en cuenta la guía propuesta con sus respectivas amenazas. Para lo cual se realizo una herramienta de software que permitiera realizar la propuesta de la guía.(ver anexo D Pruebas del framework de seguridad informática)

Luego se procedió a asociar dichas amenazas identificadas en la guía resultado del objetivo 1, ver anexo A, con los riesgos identificados en cada fase del ciclo de vida del APT.

Introducción

Posteriormente se asociaron un conjunto de buenas prácticas y herramientas para mitigar la fuga de información ocasionada por APT que surgieron del objetivo 2 y 3. Ver anexo B y C que aplican a cada riesgo idenficado para cada uno de esas fases.

Cabe anotar que las pruebas del framework permitió identificar del hospital quilisalud un grupo de activos sensibles a fuga, un conjunto de buenas prácticas y herramientas para mitigar la fuga de información ocasiona por APT en los activos informáticos del sector hospitalario y en ningún caso se ejecutaron ataques APT para ver la funcionalidad de este, ya que en las herramientas que el framework propone son resultado de investigación enfocadas en prevenir APT de autores reconocidos que fueron tomadas como referencia y clasificadas según su nivel de protección. Es de resaltar que a todas las herramienta se le realizaron las pruebas pertinentes para combatir las amenazas asociadas a las APT que tienen vector de ataque correo electrónico y se monto el ambiente de pruebas para prevenir fuga de información . **Ver anexo D**. (Pruebas del framework de seguridad informática) Es por ello que el framework se enfoco en que las entidades hospitalarias reduzcan los riesgos de que suceda un hecho de tal envergadura que pueda causar daño en su imagen y fuga de información en activos delicados y sucectibles a ser protegidos.

Introducción

3. Resultados

3.1. Guía (Propuesta de identificación de activos sensibles del sector hospitalario vs amenazas persistentes que aprovechan vulnerabilidades cuyo vector de infección es el correo electrónico).

En esta sección fué posible diseñar una guía (ítem 3.1.4) para el levantamiento de activos sensibles a fugas de información ocasionadas por APT provenientes de correo electrónico, la cual busca apoyar el sistema de gestión de seguridad de la información, para que la entidad pueda corregir políticas, procedimientos, objetivos y acciones encaminadas a garantizar la confidencialidad de los activos de información, y mantener el nivel de riesgo en un nivel aceptable. En esta guía es posible identificar las amenzas a las que pueden estar expuesto sus activos sensibles y ver las vulnerabilidades (Ver ítem 3.1.17, tabla 23 clasificación nivel de fuga de información) que puede aprovechar un APT.

Para dar respuesta al objetivo 1 que corresponde al proceso de identificar los activos sensibles en el sector hospitalario se debe contar con un responsable líder de la actividad, que en lo posible tenga conocimiento sobre estándares de gestión de seguridad de la información como la norma ISO 27001:2013. Para la cual se creó una guía en esta sección ítem 3.1.4 e inicia con deficiones expuestas a partir del ítem 3.1.3, dicha guía define los pasos a seguir para realizar el levantamiento de activos y que va permitir identificar las amenazas a los que esta expuesto cada uno de los activos de la organización que tienen información delicada. Asi mismo fue posible definir los roles que se deben involucrar en el proceso, el diseño de la propuesta de valoración de activos y amenazas (Ver ítem 3.1.12, tabla 15), como también se muestra la valoración de activos con vulnerabilidades (Ver ítem 3.1.12, tabla 16) usadas por las APT y por último se presenta el análisis de resultados del objetivo 1.

Introducción

3.1.3. Definición de roles en el sector hospitalario

Para facilitar la compresión de la guía a continuación se presenta la tabla 7 de especificación de roles que deben existir dentro del sector hospitalario con las responsabilidades de acuerdo a su rol.

Rol	Responsable	Responsabilidades
Propietario	Es el proceso encargado que creo la información. Es la parte de la entidad hospitalaria, un proceso, o grupo de trabajo que tiene la responsabilidad de que los activos sean clasificados de acuerdo a su uso.	-Toma decisiones sobre el uso de la información. -Garantiza que se cumplan los controles de protección de la información. -Garantiza el acceso a las personas de acuerdo a su rol como también que la información se encuentre disponible e integra.
Custodio	Es el área encargada de la custodia de la información para efectos de permitir su acceso. Designado para hacer efectivas las restricciones y clasificaciones de acceso definidos por el propietario. Los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original	-Cumplir con los controles estipulados para la protección de la información. -Ejecutar las actividades propias de su cargo, de acuerdo a la custodia de la información.
Usuario Final	Es la persona que hace uso de los activos de información	-Hacer uso de los activos de información. -Garantizar la confidencialidad, integridad y disponibilidad del activo de información. -Reportar cualquier evento que atente contra la seguridad de la información.
Líder del Proceso	Es el responsable de estimar los riesgos asociados a los activos, establece las políticas para prevenirlos de forma eficiente en el futuro.	-Comunicar a todos los procesos del sector hospitalario la importancia de la gestión de los activos de forma clara y precisa. -Responsable de los controles que se deben de tomar para el control de las amenazas y vulnerabilidades presentes en los sistemas de información existentes en un proceso. -Responsable del determinar el alcance del levantamiento de activos de la organización de acuerdo al nivel de protección que se le quiera dar a la información. -Responsable de la clasificación de la información de cada proceso del hospital de acuerdo a su función.

Fuente: (Colciencias, 2015), (MINTIC, 2016d).

Tabla 7. Definición de roles.

3.1.4. Diseño de la propuesta

Se propuso un diagrama de flujo para facilitar la comprensión de la guía y que la entidad hospitalaria pueda iniciar un proceso de identificación de activos sensibles, se recomienda aplicar el proceso mostrado en la ilustración 4 que permite que el líder reconozca el estado actual de la gestión de activos y pueda ubicarse en el punto específico que le corresponde

Introducción

aplicar de acuerdo con las acciones de gestión del riesgo que la entidad pudiera tener adelantadas. Es importante considerar que, para los efectos de esta guía, algunas fases son obligatorias y otras flexibles de acuerdo con lo que la entidad ya haya desarrollado. Las fases son las propuestas en la ilustración que se muestra a continuación.

Diagrama de flujo para determinar las fases que debe seguir el administrador de sistemas de acuerdo a los procesos que tiene dentro de la organización para identificación de activos. Fuente de elaboración propia.

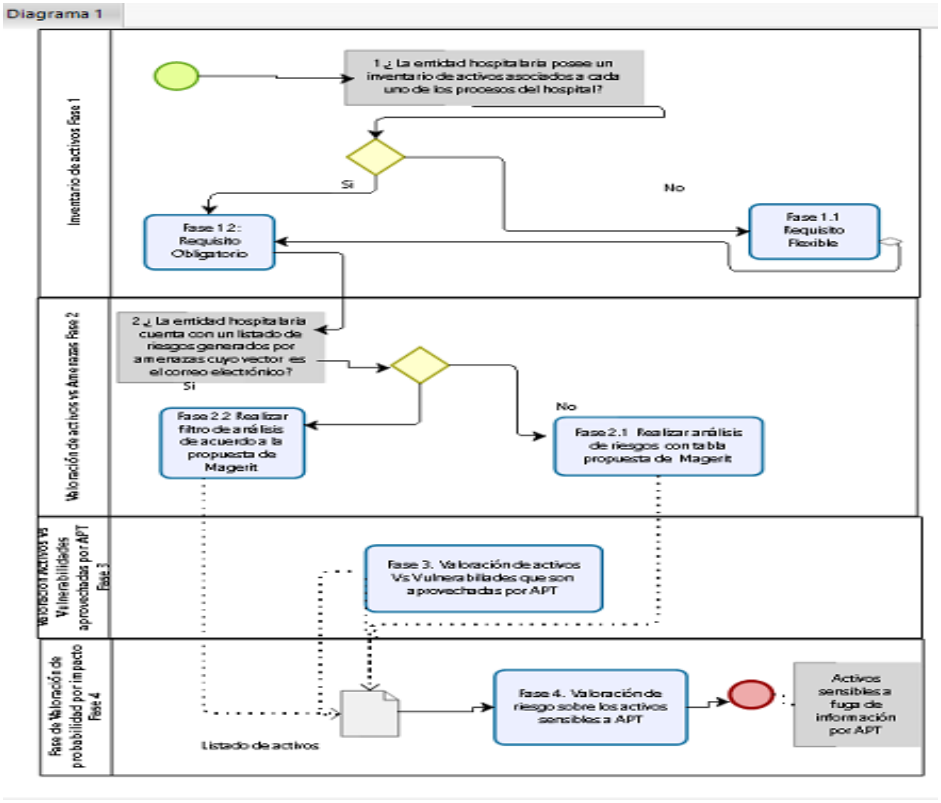


Ilustración 4. Diagrama de Flujo para levantamiento de activos.

Fuente de Elaboración Propia

3.1.5. Definición del alcance

Antes de proceder al levantamiento de activos, la entidad debe determinar los activos que hacen parte del alcance que se pretende cubrir con la gestión de riesgos posterior a esta guía. Para esto se deben establecer los procesos involucrados, las áreas organizacionales, sedes y personas que serán considerados.

A continuación, se muestra una breve descripción de lo que involucra cada una de las fases mostradas en el diagrama

Introducción

3.1.6. Fase 1. Inventario de activos

Esta fase determina cuáles son los activos sensibles a fuga de información para el alcance seleccionado. Dependiendo de su nivel de madurez dentro del levantamiento de activos, el líder puede aplicar Fase 1.1; en cambio la Fase 1.2 es obligatoria.

3.1.7. Fase 1.1: Información Flexible

En el caso de que no se cuente con un inventario de activos previamente elaborado, el líder del proceso encargado del levantamiento de activos procede a asociar la siguiente información a los activos:

-**Identificación del activo:** Consecutivo de tipo número **generalmente** único. El líder determina esta identificación. Nota: No se recomiendan números muy largos o siglas de compleja comprensión.

-**Proceso:** Identifica el activo dentro de un tipo de proceso del sector hospitalario. Se propone considerar los siguientes tipos de procesos, no obstante, la entidad es libre de definir los tipos de procesos de su mapa estratégico. Ver tabla 8**.**

Misional	**Estratégicos**	**Apoyo**	**Evaluación y mejora**
Son aquellos que son fundamentales para que la entidad hospitalaria preste sus servicios, razón por la cual son considerados fundamentales.	Son aquellos que establecen políticas, estrategias, fijación de objetivos. Son considerados factores clave o estratégicos dentro de la entidad hospitalaria.	Son el soporte de los procesos estratégicos, misionales, monitoreo y evaluación. Su función es estar dirigidos a la provisión de los recursos para que los demás procesos funcionen bien.	Son aquellos procesos indispensables para medir y realizar recopilación de la información, que por lo general es usada para medir el desempeño, y mirar acciones de mejora en pro de la entidad hospitalaria. Son una parte integral de los procesos estratégicos, de apoyo y de los misionales

Tabla 8. Procesos del sector salud de referencia.
Fuente de elaboración Propia

-Nombre Activo: Identifica el activo con un nombre, facilita su identificación dentro del proceso.

-Descripción/Observaciones: Describe claramente el activo identificado considerando su relevancia dentro del proceso.

Introducción

-Tipo de Activo: Identifica al activo de acuerdo a la información que gestiona. Para facilitar el proceso se sugiere a siguiente tabla:

Tipo de Activo: en este ítem el líder define el tipo al cual pertenece el activo. Para facilitar el proceso se deben de considerar la clasificación de la tabla 4, se debe de señalar con X, en el anexo:

Identificador	Categoría	Ejemplo
STI	Servicios TI	De estos hacen parte las aplicaciones y la infraestructura TI.
DAT	Datos / Información	Conformados por las bases de datos, archivos de datos y contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario de la entidad hospitalaria.
SW	Software	Conformados por las aplicaciones, los sistemas operativos, y las herramientas de desarrollo al igual que los utilitarios.
HW	Hardware	Es la parte física conformada por equipos, los servidores de sistemas operativos, computadores, routers, hubs, firewalls, medio magnético
SI	Soportes de información	De estos hacen parte los discos, cintas, USB, CD, DVD.
COM	Redes de comunicaciones	Son aquellos medios de transporte que llevan información de un lado a otro.
AUX	Equipamiento auxiliar	Equipamiento de soporte a los sistemas de información.
PER	Personal/Recursos Humanos	Usuarios, proveedores, personal TI

Fuente: (Sotelo, Utrilla, & Ortega, 2012).
Tabla 9. Activos de Información

-Ubicación: Es la ubicación tanto física como electrónica del activo de información, esto con el fin de facilitar su búsqueda dentro del proceso. Es asignada generalmente por el usuario final o custodio.

-Responsabilidad del activo: Establece quién es el propietario del activo en la entidad hospitalaria. Puede ser el custodio, propietario o cliente.

-Nombre: Identifica al responsable del activo dentro de la organización.

Introducción

3.1.8. Fase 1.2: Información Obligatoria

Esta fase determina el nivel de sensibilidad a fuga de información presente en los activos identificados en la fase 1.1

A. Información Prioritaria

- **Clasificación de Activos de Información:** Para el alcance del levantamiento de activos sensibles a la fuga de información que propone esta guía, solo será contemplado el pilar de seguridad de la información asociado a la confidencialidad, que hace referencia a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados y que podría originarse por amenazas persistentes avanzadas. Para facilitar la labor del líder se definieron tres niveles alineados con los tipos de información declarados en la ley 1712 de 2014 (MINTIC, 2016d). Para facilitar el proceso se suministra la tabla 10:

Valor	Tipo de Información	Descripción
0	No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PÚBLICA RESERVADA.
1	Información pública	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
2	Información pública clasificada	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
3	Información pública reservada	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de reputación y/o económica.

Fuente:(MINTIC, 2016d).
Tabla 10. Clasificación de la información.

Formato: Si se ha señalado con una X en el punto Tipo de Activo (**Datos / Información)**, en este punto se debe de señalar con X el tipo de formato que maneja la información para

Introducción

su presentación de forma impresa o en pantalla: hojas de Cálculo, documentos de texto, PDF, presentaciones, imágenes, audio.

Atributos de los activos en cuanto a la seguridad de la información:

En esta actividad el equipo líder del sector hospitalario determina el nivel de protección adecuada, de acuerdo a los atributos de Confidencialidad, Integridad y Disponibilidad, esto significa proteger la información y los sistemas de información del acceso, uso, difusión, entorpecimiento, modificación o destrucción no autorizados, para facilitar este proceso el líder del proceso podrá realizar esta clasificación calificándolo con 0,1,2,3 de acuerdo a cada pilar como se muestra a continuación:

Disponibilidad: Propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizado. De acuerdo al momento, forma y a los recursos que necesita para ello. Para ayudar a la identificación de esto se sugiere responderse a esta pregunta ¿Cuál sería la importancia o el trastorno que tendría el que el activo si no estuviera disponible? (Meneses, 2007) (MINTIC, 2016d). Ver tabla 11.

Valor	Descripción
0	Su no disponibilidad no es relevante en la entidad hospitalaria.
1	Se debe garantizar al menos una disponibilidad del 10% del tiempo.
2	Se debe garantizar al menos una disponibilidad del 50% del tiempo.
3	Se debe garantizar al menos una disponibilidad del 100% del tiempo

Fuente: (Meneses, 2007).*Tabla 11.Disponibilidad.*

Integridad: Hace referencia a la exactitud y completitud de la información (ISO 27000), esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. Para ayudar a la identificación de esto se sugiere responderse a esta pregunta ¿Qué importancia tendría que el activo fuera alterado sin autorización ni control? (Meneses, 2007)(MINTIC, 2016d)**.** Ver tabla 12.

Valor	Descripción
0	No aplica
1	Su carencia u error no es importante dentro del proceso.
2	Se debe de garantizar que este correcto al igual que completo al menos en un 70%.
3	Se debe de garantizar que este correcto al igual que completo al menos en un 99%.

Fuente(Meneses, 2007), *(MINTIC, 2016d) Tabla 12. Integridad.*

Confidencialidad: Hace referencia a que la información no esté disponible para individuos, entidades o procesos no autorizados. Para realizar una ponderación adecuada, el criterio será

Introducción

¿Cuál es la importancia que tendría que al activo se accediera de forma no autorizada? (Meneses, 2007)(MINTIC, 2016d). Ver tabla 13.

Valor	Descripción

0	No aplica
1	Daños muy bajos, el incidente no trascendería del área afectada.
2	Los daños serian relevantes, el incidente implicaría a otras áreas.
3	Los daños serian catastróficos, la reputación y la imagen de la entidad hospitalaria se verían comprometidas.

Fuente: (Meneses, 2007). *Tabla 13. Confidencialidad.*

Criticidad:

Es un cálculo automático que determina el valor general del activo, el mensaje mostrará de forma automática. El valor máximo de las tres características determinará la criticidad del activo de información analizado.

Si todos son 0 → Criticidad 0-Nula

Si el máximo es 1 → Criticidad 1-Baja

Si el máximo es 2 → Criticidad 2-Media

Si el máximo es 3 → Criticidad 3-Alta

Clasificación del nivel de criticidad de los activos

Valor	**Criticidad**	**Descripción**
0	Nula	Sin importancia
1	Baja	De menor importancia a la organización.
2	Media	De importancia a la organización
3	Alta	De gran importancia a la organización.

Tabla 14. Nivel de criticidad.

Después de realizar el paso llamado **Atributos de los activos en cuanto a la seguridad de la información,** solo se tendrán en cuenta aquellos cuya criticidad es **Media y Alta,** puesto que estos activos son los más sensibles a una posible fuga de información que pueden provenir de correo electrónico. Estos serán valorados en el Fase 2. Para facilitar el registro de información de la **Fase 1.1** y la **Fase 1.2** se propone un formato en Excel para facilitar al

Introducción

líder del proceso, hacer el inventario de activos y determinar el nivel de criticidad del activo. Ver Anexo A, ítem 6.1.

3.1.9. Fase 2: Valoración de Activos Vs Amenazas

En la **fase 1**, se determinó el análisis de criticidad de los activos, los únicos que pasan a ser valorados de acuerdo con su criticidad serán los que tengan una calificación en **Medio y Alto**.

En la **fase 2** y en el contexto de este trabajo se considerarán los diferentes tipos de amenazas a las cuales están expuestos los activos de información y que causan fuga de información usando el vector de ataque correo electrónico. Defínase como amenaza algo que puede afectar a uno a más activos de la entidad y que puede estar asociada a una vulnerabilidad que podría ser aprovechada por los atacantes para ejecutar un ataque persistente avanzado en el sistema y ocasionar fuga de información.

A continuación, se presenta una clasificación de las amenazas de acuerdo a MAGERIT en la cual se realizó una compilación de amenzas y se mapeo teniendo en cuenta a MAGERIT V.3 (ver tabla 15, en esta sección. Clasificación de amenázas), al final se tomo como referencia este estándar al hacer una homolagacion de amenazas que apuntan a fuga de informacion y que no esta presente en otros estándares. En sisntesis las amenazas que fueron extraídas fueron adaptadas para mitigar ataques que tienen vector de ataque el correo electrónico. A continuación, se muestran las amenazas que apuntan al correo electronico. Ver tabla 61. Para la cual se diseño un artefacto ver Anexo A, Item 6.1

Clasificación de las Amenazas según Margerit.

Nombre de la Amenaza	Nombre del Activo	Descripción
Errores del administrador [EA]	[DAT] datos / información [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información	Son aquellos que hacen referencia a las posibles equivocaciones que de forma intencional o no puede tener un administrador al momento de instalar u operar el sistema que está bajo su responsabilidad.
Errores de [re-]encaminamiento [ERE] CORREO	[SW] aplicaciones (software) [COM] redes de comunicaciones	Son aquellos que hacen referencia al envío de datos usando un sistema o una red y que de forma intencional o no hagan un desvió de información a otro sitio; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. A veces el error de encaminamiento supone un error de entrega, puesto que la información acaba en manos de quien no tiene ningún permiso para ello.
Fugas de información [FI]	[DAT] datos / información [SW] aplicaciones [COM] comunicaciones (tránsito) [SI] soportes de información [PER] personal (revelación)	Son aquellos que hacen referencia a revelar por indiscreción verbal o por medios electrónicos, soporte papel, información de la entidad hospitalaria.
Suplantación de la identidad del usuario [SI]	[DAT] datos / información [SW] aplicaciones (software) [COM] redes de comunicaciones	Son aquellos que hacen referencia a cuando un atacante se hace pasar por un usuario, disfrutando de los privilegios de este. Generalmente es perpetrada por personal interno de la compañía, aunque en muchos casos también hay personal externo.
Usuarios Privilegiados [AP]	[DAT] datos / información [SW] aplicaciones (software) [HW] equipos informáticos (hardware)	Son aquellos que hacen referencia a que un usuario disfruta de un nivel de privilegios para un determinado propósito y en la gran mayoría de veces abusa de esto con otros fines dentro de la entidad hospitalaria.
Interceptación de información (escucha) [INE]	[COM] redes de comunicaciones	Son aquellos que hacen referencia a cuando el atacante tiene acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
Ingeniería social [ES]	[PER] equipamiento auxiliar	Son aquellos que hacen referencia al abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Fuente: Elaboración propia adaptada de (Ministerio de Hacienda y Administraciones Públicas, 2012)(Sotelo et al., 2012). *Tabla 15. Muestra la clasificación de las amenazas de acuerdo a MAGERIT V.3*

3.1.10. Fase 2.1 Realizar análisis de riesgos con tabla propuesta de Magerit

Si no posee este listado de riesgos cuyo vector es el correo electrónico; se sugiere a realizar un análisis de riesgo valorando las amenazas sugeridas en la tabla 15.

3.1.11. Fase 2.2 Realizar filtro de análisis de acuerdo con la propuesta de Magerit

Aquí se pretende disponer de un listado de riesgos cuyo vector es el correo electrónico; esto puede extraerse de un análisis de riesgos, por lo cual, si la entidad ya lo ha realizado, debe aplicar un filtro de los riesgos asociados con las amenazas cuyo vector es el correo electrónico, presentadas en la tabla 15.

Los activos de la fase 1 donde la criticidad es **ALTA y MEDIA,** serán valorados frente al riesgo cuyo vector es el correo electrónico.

Para realizar dicha valoración se presenta el siguiente formato en Excel para facilitar la labor del líder del proceso. Ver tabla 17 Anexo A, ítem 6.1.

Nota: Para la fase 4 de valoración de riesgo (probabilidad por impacto) se tendrán en cuenta los activos que presenten al menos alguna marca (X) entre los tipos de amenaza de la tabla 12.

3.1.12. Fase 3 Valoración de activos vs vulnerabilidades explotadas por APT

En esta fase a partir del análisis de la **FASE 1**, Se realiza el filtro que considera aquellos activos donde la criticidad es **ALTA y MEDIA** y cuyo atributo de seguridad comprometido es la **Confidencialidad**, el listado de activos resultantes de esta fase, sarán valorados con respecto a las amenazas identificadas en la **FASE 2** cuyo vector de ataque es el correo electrónico. En la **FASE 3** se tendrá en cuenta el filtro de la **FASE 1** y serán valorados los activos sensibles a fuga de información frente a las vulnerabilidades explotadas por APTs que utilizaron el vector de ataque correo electrónico según lo presentado en la ilustración 10, además se presenta un artefacto en la ilustración 11, que permite valorar los activos de la fase 1 frente a estas vulnerabilidades.

Para facilitar el proceso de identificación de las vulnerabilidades a las que están expuestas los activos se recomienda realizar el siguiente checklist; que fue elaborado a partir de la identificación de vulnerabilidades explotadas por las amenazas persistentes avanzadas y

que tienen su correspondiente CVE. Se hará un filtro en especial a activos de información de cualquier tipo, identificados en la **FASE 1,** teniendo en cuenta la tabla 16**.**

Tabla 16.Vulnerabilidades usadas por APT.

Listado de activos	Es un activo que tenga instalada al menos alguna de las versiones de Microsoft Office sea inferior a 2002	Es un activo que tenga instalado al menos alguno de los siguientes sistemas operativosWindows 2000, server 2003, 2008, vista y XP	Es un activo que use para su servicios Adobe Reader y Acrobat con una version inferior a 10.X independiente del sistema operativo (Windows, Linux, Macintosh)	Es un activo que use para sus servicios el motor de bases de datos Microsoft SQL Server 2000 SP4, 2005 SP4, y 2008 SP2, SP3 y R2; o activos que usen Microsoft BizTalk Server 2002 SP1; o Microsoft Commerce Server 2002	Es un activo que halla usado en algunas de las aplicaciones Oracle Java SE	Es un activo que use para sus servicios Microsoft Windows Vista SP2 and Server 2008 SP2	Es un activo que use para sus servicios Microsoft Office 2007 SP3, 2010 SP2, SP1 2013, y 2013 RT SP1	Es un activo que tenga implementado un servicio en Python 2.7.14	Tiene instalada alguna versión de servicio web basado en Internet Information Services (IIS) o Apache

Nota: *Para la fase 4 de valoración de riesgo (probabilidad por impacto) se tendrán en cuenta los activos que presenten al menos alguna marca (X) en las vulnerabilidades según el tipo de activo mostrado en la ilustración 11*.

3.1.13. Fase 4. Fase de Valoración de Probabilidad por Impacto.

Una vez la entidad cuente con el listado de activos identificados en la Fase 2 y Fase 3, se sugiere realizar lo siguiente para cada uno de los activos:

-Determinar la probabilidad de que se materialice la amenaza, a partir de la revisión de muchas guías de buenas prácticas se sugiere la tabla 17, la cual puede ser modificada según las reglas del negocio:

Probabilidad

Valor	Rango	Descripción	Frecuencia
0	Improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años

1	Posible	El evento podría ocurrir en algún momento	Al menos dos veces en los últimos 2 años.
2	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez en el último año
3	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Tabla 17. Probabilidad de ocurrencia.

-Determinar el impacto de que se materialice la amenaza, a partir de la revisión de muchas guías de buenas prácticas se sugiere la tabla 18 la cual puede ser modificada según las reglas del negocio.

Valor	**Rango**	**Descripción**
0	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad hospitalaria
1	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad hospitalaria
2	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efecto sobre la entidad hospitalaria
3	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efecto sobre la entidad hospitalaria

Tabla 18. Calcular el Impacto.

-S**ensibilidad del activo:** En esta fase el líder determina el nivel de sensibilidad de activo de acuerdo con la siguiente fórmula:

Sensibilidad=NroAmenazas*(0,3)+NroVulnerabilidades*(0,7).

Al realizar este cálculo usando los factores 0,3 y 0,7; se da mayor prioridad el asociado a 0,7 que está asociado a las vulnerabilidades que pueden presentar dichos activos.

Los resultados son valores contemplados en la siguiente ilustración y que sirven de insumo para calcular el nivel de sensibilidad: ver tabla 19.

Valor	Descripción	Nivel de sensibilidad
1	Inferior	0 a 2,3
2	Bajo	2,4 a 4,8
3	Medio	4,9 a 7,2
4	Alto	7,3 a 9,6
5	Superior	9,7 a 12

. *Tabla 19. Sensibilidad del activo. Fuente de elaboración propia*

Nivel fuga de información: Calcula el nivel de riesgo asociado al activo para determinar el nivel fuga de información cuyo vector de ataque es el correo electrónico del activo:

Niveldefugainformacion=Probabilidad*Impacto+Sensibilidad del activo

Nombre Activo	Probabilidad	Impacto	Sensiblidad del activo	Nivel de fuga de información
	3	3	2,3	11,3

Tabla 20. Determinar el nivel de fuga de información Fuente de elaboración propia.

A partir del nivel de fuga de información ocasionada por un APT cuyo vector de ataque es el correo electrónico se determinará el nivel de protección que se le debe de suministrar al activo mediante controles. Ver tabla 21.

Nivel de fuga de información	Nivel de riesgo
>=15	Alto
>7 y <14	Medio
>7	Bajo

.

Tabla 21. Clasificación Nivel de Fuga de Información

3.1.14. Revisión.

El líder del proyecto, en esta fase realiza la verificación, que le permite llevar a cabo si un activo de información continúa o no siendo parte del inventario.

Este proceso de inventario puede ser revisado o validado en cualquier momento, por el líder del proceso. Las razones para realizar una revisión al inventario son: actualizaciones al

proceso al cual está asociado el activo, inclusión de nuevos registros ya sea de calidad u otros procesos, adicción de un nuevo activo, retiro de un activo, cambio de políticas de seguridad en un activo en específico, adicción de nuevas amenazas proveniente de correo electrónico, adicción de nuevas vulnerabilidades de las cuales se aprovechan las amenazas persistentes avanzadas, cambios en la valoración de probabilidad por impacto según las reglas del negocio actual, cambios en el nivel de criticidad de los activos, cambios en alguna política interna de la compañía que afecte el levantamiento de activos (MINTIC, 2016a).

3.1.15. Actualización

Cada vez que se definan cambios en el inventario o ya exista un inventario de amenazas se recomienda iniciar desde la Fase 1 y para poder garantizar una trazabilidad completa de todo el activo.

3.1.16. Publicación

El inventario de activos de información debe ser un documento clasificado como "Confidencial", y no debe tener características que lo permitan modificar por los usuarios autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso.

3.1.17. Determinacion de la fase mas sensible a fuga de informacion:

Despues de la realización de los diferentipos tipos de ataques de amenazas persistentes avanzadas, la gran mayoría usaron la técnica del spear-phishing, de la cual se considera puede mostrar una o más de las siguientes características:

- Es una amenaza mixta → Es una combinación de correo electrónico, URL dinámicas y descargas directas.
- Uso de vulnerabilidades de día cero → Este tipo de ataques aprovechan vulnerabilidades de día cero presente en los navegadores, complementos y aplicaciones de escritorio.

- Ataque en varias etapas→ El reconocimiento es la primera etapa de un ataque APT que involucra etapas posteriores de comunicaciones salientes de malware, descargas binarias y exfiltración de datos.
- Falsificación de correo electrónico→ Las amenazas de correo electrónico de spearphishing generalmente están dirigidas a individuos, por lo que no se parecen mucho al correo basura de gran volumen que inunda Internet, haciendo que las protecciones tradicionales de correo electrónico sean ineficaces (FireEye, 2016a).

Como se mencionó anteriormente un ataque de spear-phishing usa el correo electrónico dirigido a un destinario previamente estudiado, el cual es atraído a descargar un archivo aparentemente inofensivo o hacer clic en un enlace malicioso o cargado de exploits. El archivo, a menudo un exploit de vulnerabilidad, instala un malware en el computador comprometido. El malware accede un servidor malicioso de comando y control a la espera de instrucciones de un usuario remoto. Al mismo tiempo, usan un documento como señuelo que se abrirá cuando el cliente ejecuta malware o exploit para ocultar la actividad maliciosa (Trend Micro, 2012).

El spear phishing es una herramienta que se ha utilizado en grandes campañas de APT, como Carbanak o BlackEnergy, Bad Rabbit, que comenzaron con una infección vía email (Lab, 2017). Los correos electrónicos de Spear-phishing pueden tener archivos adjuntos de diferentes tipos de archivo. Los más comúnmente usados son por ejemplo: .XLS, .PDF,.DOC, .DOCX y .HWP (Trend Micro, 2012)(Li et al., 2016).

Se mostrará un listado de las vulnerabilidades aprovechadas por los APT que aprovecharon el vector de ataque correo electrónico, donde se parte de los CVE de cada uno de los ataques y el tipo de vulnerabilidad que esta aprovecho, se tuvo en cuenta algunos de los ataques de APT que se indican a continuación ver tabla 22.

Lista de Vulnerabilidades aprovechadas por las APT.

CVE	Nombre APT	Tipo de Vulnerabilidad
CVE-2009-3129	Octubre Rojo	Ejecutar código en la memoria
CVE-2009-31297	Shady-RAT	Deficiencia en el proceso de negociación en el protocolo TLS y el protocolo SSL.
CVE-2010-2743	Stunext	Fallo cola de impresión (MS10-61)
CVE-2010-3332	Octubre Rojo, Oak Ridge National Laboratory	Divulgación de información
		Mediante Propiedad Control.View State
CVE-2011-1353	Nitro	Error en el modo de acceso a las claves de registro de Adobe Reader.
CVE-2011-2431	Nitro	Error de validación de entrada
CVE-2011-2432	Nitro	Desbordamiento de bufer
CVE-2011-2433	Nitro	Desbordamiento de búfer
CVE-2011-2434	Nitro	Desbordamiento de búfer
CVE-2011-2439	Nitro	Condición de vulnerabilidad de fuga de memoria
CVE-2011-2440	Nitro	Error al analizar archivos PDF corruptos
CVE-2011-2441	Nitro	búfer basado en pila en Cool Type
CVE-2011-2442	Nitro	Vulnerabilidad de error de lógica
CVE-2011-3402	Duqu	Motor de análisis de fuentes TrueType en win32k.sys
CVE-2011-3544	Shady-RAT	Error de validación de entrada java
CVE-2012 -0158	Octubre Rojo, Carbanack	Corrupción de Memoria
CVE-2012-0507	APT1, APT3	Java Atomic Reference Array
CVE-2012-2539	Shady-RAT	Corrupción de memoria
CVE-2013-3906	Carbanack	Desbordamiento de enteros
CVE-2014-1761	Carbanack, Shady -RAT	Corrupción de Memoria. Confusión Objeto. RTF override table
CVE-2018-1000030	Orangeworm	Heap-Buffer-Overflow, Heap-Use-After-Free.
CVE-2018-4889	Orangeworm	Error de Buffer
CVE-2015-2545	Carbanack	Formato incorrecto EPS (PostScript encapsulado)

Tabla 22.listado de las vulnerabilidades aprovechadas por los APT

Fuente de elaboración propia

En el siguiente listado se mostró los APT y los sistemas(activos) que afectan y la valoración del impacto

CVE	Nompre APT	Sistemas que Afecta	Valoración Impacto
CVE-2009-3129	Octubre Rojo	Microsoft Office Excel 2002, Microsoft Office Excel 2003, Microsoft Office Excel 2007, Microsoft Office 2004 para Mac, Microsoft Office 2008 para Mac, Convertidor de archivos con formatos XML abiertos para Mac y todas las ediciones compatibles de Microsoft Office Excel Viewer y Paquete de compatibilidad de Microsoft Office	9
CVE-2009-31297	Shady-RAT	Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 , OpenSSL before 0.9.81, GnuTLS 2.8.5, Mozilla Network Security Services (NSS) 3.12.4 productos Cisco y otros	8,6
CVE-2010-2743	Stunext	Windows 2000, server 2003, 2008, vista y XP	7,2
CVE-2010-3332	Octubre Rojo, Oak Ridge National Laboratory	Internet Explorer Microsoft .NET Framework ASP.NET. Microsoft SharePoint Services de 64 bits 2.0 de Microsoft SharePoint Services 3.0 SP2 de Microsoft SharePoint Services 3.0 SP1 de Microsoft SharePoint Server 2010 Standard Edition 0 Microsoft SharePoint Server 2010 Enterprise Edition 0 Server 2007 Microsoft SharePoint x64 SP2 de Microsoft SharePoint Server 2007	5
CVE-2011-1353	Nitro	Adobe Reader X (10.1) y 10.x anteriores versiones para Windows y Macintosh Reader 9.4.5 y versiones anteriores a 9.x de Adobe para Windows, Macintosh y UNIX Adobe Reader 8.3 y versiones 8.x anteriores para Windows y Macintosh Adobe Acrobat X (10.1) y 10.x anteriores versiones para Windows y Macintosh 9.4.5 y versiones anteriores a 9.x de Adobe Acrobat para Windows y Macintosh Adobe Acrobat 8.3 y versiones 8.x anteriores para Windows y Macintosh	6,9
CVE-2011-2431	Nitro	Adobe Reader y Acrobat	6,8
CVE-2011-2432	Nitro	Adobe Reader y Acrobat	9,3
CVE-2011-2433	Nitro	Adobe Reader y Acrobat 8	9,3
CVE-2011-2434	Nitro	Adobe Reader y Acrobat 10	9,3
CVE-2011-2439	Nitro	RedHat Enterprise Linux, Adobe Reader	9,3
CVE-2011-2440	Nitro	Adobe Acrobat Reader en Macintosh Microsoft Windows 7 Microsoft Windows Server 2008 Microsoft Windows Vista de Microsoft Windows Server 2003 de Microsoft Windows XP Microsoft Windows 2000	6,8
CVE-2011-2441	Nitro	Adobe Reader	9,3
CVE-2011-2442	Nitro	Adobe Reader X (10.1) y versiones anteriores para Windows y Macintosh, Adobe Reader 9.4.2 y versiones anteriores para UNIX y Adobe Acrobat X (10.1)	
CVE-2011-3402	Duqu	Microsoft Windows XP SP2 y SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2 y R2 SP1 y Windows 7 Gold y SP1	9,3
CVE-2011-3544	Shady-RAT	linux windows osx Xerox FreeFlow Print Server (FFP)	10
CVE-2012 -0158	Octubre Rojo, Carbanack	Apple, Mail, OS x, Microsoft Office 2003 SP3, 2007 SP2 y SP3, y 2010 Gold y SP1; 2003 Web Components de Microsoft Office Service Pack 3; Microsoft SQL Server 2000 SP4, 2005 SP4, y 2008 SP2, SP3 y R2; * Microsoft BizTalk Server 2002 SP1; * Microsoft Commerce Server 2002	10
CVE-2012-0507	APT1, APT3	Oracle Java SE	10
CVE-2012-2539	Shady-RAT	Microsoft Windows Microsoft Office Microsoft Server Software Internet Explorer	9,3
CVE-2013-3906	Carbanack	Microsoft Windows Vista SP2 and Server 2008 SP2; Office 2003 SP3, 2007 SP3, 2010	9,3
CVE-2014-1761	Carbanack, Shady	Microsoft Office 2010 SP2 English on Windows 7 SP1 English SO. Windows	9,3
CVE-2015-2545	Carbanack	Microsoft Office 2007 SP3, 2010 SP2, SP1 2013, y 2013 RT SP1	9,3
CVE-2015-1701	APT28(Operation	Microsoft Windows Server 2003 SP2, Vista SP2 y Server 2008 SP2	7,2
CVE -2017-0199	TA459 APT	Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2,	9,3
CVE-2014-4114	Sandworm		
CVE-2018-1000030	OrangeWorm	Python 2.7.14	8,1
CVE-2018-4889	OrangeWorm	Adobe Acrobat Reader 2018	6,5

Tabla 23. APT vs

Sistemas afectados
Fuente de elaboración propia

En conclusión con los estudios realizados con anterioridad, se identificó que la fase más crítica y sensible de un ataque APT es la fase de distribución o más conocida como entrega en el modelo de Kill Chain, debido a que es donde un usuario sin conocimientos y educación ante esta amenaza latente puede ejecutar el malware que se envió a través del vector de ataque correo electrónico con solo abrir un documento adjunto recibido de un destinatario desconocido o por medio de una cadena de correos. En ese orden de ideas es donde se debe identificar el problema y detener el proceso.

3.1.18. Analisis de Resultados

-Se logro determinar el nivel de sensibilidad de los activos, haciendo prioridad en las vulnerabilidades al cual está expuesto y por el cual puede ser objeto de una amenaza persistente avanzada.

-El cálculo de la sensibilidad del activo permite determinar el nivel de fuga de información y así determinar las políticas para protección de los activos.

-Análisis de vulnerabilidades más de las que se aprovechan las amenazas persistentes avanzadas.

-La valoración de activos sensibles a fuga de información permite a la entidad de salud determinar el nivel de exposición a que se encuentran, expuestos los activos del sector.

- Aplicar una guía sistemática para la identificación de activos sensibles a fugas de información en el sector salud permite enriquecer el análisis de riesgos de seguridad de la información y plantear controles de mitigación enmarcados en un plan de tratamiento y permite identificar cuáles son las vulnerabilidades más comunes de las que se aprovechan las amenazas persistentes avanzadas.

3.2. Buenas prácticas y herramientas para mitigar fuga de información proveniente del vector de ataque correo electrónico, de acuerdo al ciclo de vida de las APT.

Este capítulo se enfoca en mostrar la forma de operar de las amenazas persistentes avanzadas, reconociendo el ciclo de vida y se entrega un listado de buenas prácticas basados en el ciclo de vida de las amenazas persistentes avanzadas al igual que tambien basadas en las politicas y buenas prácticas de diferentes autores, normas y estandares nacionales e internacionales.

Es ta sección veremos el resultado de las buenas prácticas y herramientas asociadas al ciclo de vida de las amenazas persistente avanzadas, las cuales le permitirán al sector salud un uso eficiente de sus recursos TI; le permitirán un camino hacia la mejora de sus servicios dando un valor agregado al servicio, puesto que permitirá de acuerdo a la fase del ciclo de vida de las amenazas persistentes avanzadas gestionar los riesgos asociados forma eficiente minimizando el impacto que estas puedan sufrir por un ataque.

3.2.1. Riesgos presentes en cada fase del ciclo de vida del APT.

A partir del estudio del ciclo de vida se hizo un análisis de los riesgos presentes en cada uno de las fases, los cuales se muestran a continuación fase por fase, se hizo una selección de 13 artículos que usaban el modelo de Kill Chain (Ver anexo C, ítem 6.3, tabla 74) y a partir de la revisión se hizo un listado de riesgos mencionados por el autor y otra columna donde se hace la homologación para facilitar la comprensión por parte del lector.
Los autores son los siguientes 1. Informe_Anual_PandaLabs_2017, 2. (Luh et al., 2017), 3.(Giura & Wang, 2013), 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Crowe, W, 2015), 9. (Al-Mohannadi, Mirza, Namanya et al., 2016), 10. (Christensen, 2013), 11.

(Ioannou, Louvieris, Clewley, & Powell, n.d.), 12. (Bodeau & Graubart, 2013), 13. (Lockheed, 2014).

A continuación se muestran los riesgos asociados a cada fase del ciclo de vida del APT.

-Fase de reconocimiento

Fases	Riesgos mencionados por autor	Riesgos homologados	Autores												
			1	2	3	4	5	6	7	8	9	10	11	12	13
Reconocimiento	Robo de identidad / fraude	Suplantacion de identidad								x					
	Descubrir servidores orientados a Internet	Identificar activos objetivo													x
	DDOS	DDOS								x					
	Pruebas de servicio	Escaneo de vulnerabilidades											x		
	Phishing	Suplantacion de identidad								x					
	Ingenieria social	Ingeniería social							x	x			x		
	Buscar información de actas de congresos, listas de correo	Ingeniería social						x		x	x				x
	Busqueda, identificación y selección de objetivos	Ingeniería social						x						x	
	Fisgoneo o buscar en la basura	Footprinting				x					x				
	Recolección de correos de usuarios	Footprinting		x			x			x	x				x
	Sitios Vulnerables	Analisis de vulnerabilidades					x								
	Investigación, identificación	Ingeniería social	x				x							x	
	Selección de objetivos (direcciones IP, emails, nombres,	Footprinting													
	Escaneo de red	Footprinting							x				x		
	Mapeo de red	Footprinting							x						
	Identificar vulnerabilidades	Escaneo de vulnerabilidades		x	x	x						x			
	Perfilar Empleados	Ingeniería social y Footprinting													x

Tabla 24. Riesgos fase de reconocimiento

1. Informe_Anual_PandaLabs_2017, 2. (Luh et al., 2017), 3.(Giura & Wang, 2013), 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Crowe, W, 2015), 9. (Al-Mohannadi, Mirza, Namanya et al.…, 2016), 10. (Christensen, 2013), 11. (Ioannou, Louvieris, Clewley, & Powell, n.d.), 12. (Bodeau & Graubart, 2013), 13. (Lockheed, 2014).

Los riesgos más resaltados en la fase de Reconocimiento son la Ingeniería Social, el Footprinting y escaneo de vulnerabilidades.

-Militarización

Fases	Riesgos mencionados por autor	Riesgos homologados	Autores												
			1	2	3	4	5	6	7	8	9	10	11	12	13
Militarización	Fuerza bruta	Fuerza bruta											x		
	Preparar el payload para entrega	Backdoor								x	x				x
	Spear Phishing	Phishing							x	x			x		
	Watering Hole attacks (web de confianza infectada)	Sitios maliciosos							x						
	Sitio malicioso	Sitios maliciosos							x						
	Rootkits	Malware				x									
	Exploit 0 days	Vulnerabilidad cero days		x	x	x		x						x	
	Acomplamiento de troyanos	Malware						x							
	Backdoor	Malware		x						x				x	x
	Descargas de Drive-by, Kits de explo	Herramienta maliciosa de entrega								x					x
	Servicios maliciosos	Programa malicioso		x											
	USB infectada	Malware								x					
	Malware	Malware		x						x	x			x	
	Troyano que contenga un exploit payloads	Malware y Backdoor	x	x		x	x		x		x				

Tabla 25. Riesgos fase de militarización

1. Informe_Anual_PandaLabs_2017, 2. (Luh et al., 2017), 3.(Giura & Wang, 2013), 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Crowe, W, 2015), 9. (Al-Mohannadi, Mirza, Namanya et al.…, 2016), 10. (Christensen, 2013), 11. (Ioannou, Louvieris, Clewley, & Powell, n.d.), 12. (Bodeau & Graubart, 2013), 13. (Lockheed, 2014).

Los riesgos más resaltados en esta fase son el Malware, Backdoor y las vulnerabilidades del día cero como también el phishing.

-Fase de Distribución

Fases	Riesgos mencionados por autor	Riesgos homologados	Autores											
Distribución	Malware por medio de servidor C&C	Distribución de malware desde equipos remotos						x						
	Descargas de Drive	Sitios maliciosos							x					
	Rootkits	malware												
	Dispositivos USB infectados	Dispositivos infectados					x	x	x					
	Payload Malicioso	Backdoor					x							
	Sitios Vulnerables	Vulnerabilidades conocidas	x	x									x	
	Archivos adjuntos de correo electrónico	Phishing												x
	Archivos adjuntos Infectados	Dispositivos infectados											x	
	Send spear Phishing email	Phishing		x	x	x	x		x	x				
	Enviar correos electrónicos personalizados	Phishing			x				x					x
	URL Maliciosa	Sitios maliciosos			x	x				x				
	Bots	Dispositivos infectados					x							
	Herramienta automatizada para lanzar ataque	Herramienta maliciosa de entrega						x				x		
	Entrega del payload sobre servidores web	Backdoor												x
	Transmisión del arma al objetivo	Herramienta maliciosa de entrega						x						
	Sitio malicioso	Sitios maliciosos					x	x						x
	Troyano	Malware			x	x								

Tabla 26. Riesgos fase de distribución

1. Informe_Anual_PandaLabs_2017, 2. (Luh et al., 2017), 3.(Giura & Wang, 2013), 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Crowe, W, 2015), 9. (Al-Mohannadi, Mirza, Namanya et al.…, 2016), 10. (Christensen, 2013), 11. (Ioannou, Louvieris, Clewley, & Powell, n.d.), 12. (Bodeau & Graubart, 2013), 13. (Lockheed, 2014).

Los riesgos más resaltados en esta fase son Dispositivos infectados, sitios maliciosos y Phishing.

-Explotación

Fases	Riesgos mencionados por autor	Riesgos homologados	Autores												
			1	2	3	4	5	6	7	8	9	10	11	12	13
Explotación	Reconocimiento interno	Escalar privilegios												x	
	Payload malicioso ejecutado	Backdoor y Malware													
	Botnet	Dispositivos infectados							x						
	Malware	Malware							x						
	Escaneo Interno de red	Escaneo de vulnerabilidades			x										
	Inyección Sql	Vulnerabilidades conocidas				x				x			x		
	Recolección de Credenciales de usuario	Recolección de Credenciales de usuario			x										
	Explotación de una aplicación o vulnerabilidad del sistema operativo	Vulnerabilidades conocidas						x		x					
	Explotar máquinas de empleados	Explotar equipos		x	x			x		x					
	Código malicioso ejecutado	Dispositivos infectados	x	x				x							
	explotar la vulnerabilidad elegida	Vulnerabilidades conocidas													

Tabla 27. Riesgos fase de explotación

1. Informe_Anual_PandaLabs_2017, 2. (Luh et al., 2017), 3.(Giura & Wang, 2013), 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Crowe, W, 2015), 9. (Al-Mohannadi, Mirza, Namanya et al.…, 2016), 10. (Christensen, 2013), 11. (Ioannou, Louvieris, Clewley, & Powell, n.d.), 12. (Bodeau & Graubart, 2013), 13. (Lockheed, 2014).

Los riesgos más resaltados en esta fase son vulnerabilidades conocidas, explotar equipos.

-Instalación

Fases	Riesgos mencionados por autor	Riesgos homologados	Autores												
			1	2	3	4	5	6	7	8	9	10	11	12	13
Instalación	Instalar malware de forma remota (backdoor /	Ejecución de malware en maquinas de usuarios que son el objetivo											x		x
	Inyección de código	Vulnerabilidades conocidas								x					
	Instalar Backdoor	Programa malicioso				x									
	Suplantación de identidad	Phishing								x					
	Escalar privilegios de acceso	Escalar privilegios	x	x	x										
	Ubicar usuarios con privilegios	Recolección de Credenciales de usuario		x	x										
	Ocultamiento de malware	Esteganografia				x			x						
	Botnet	Red Infectada							x						
	Backdoor	Backdoor	x			x									
	Descargar software malicioso	Ejecución de malware en maquinas de usuarios que son el objetivo					x			x	x				x
	Dominio Malicioso	Sitios maliciosos					x								
	Instalar malware adicional	Instalacion y ejecucion de programas en segundo plano (Backgroud)					x			x	x				
	backdoor instalado en maquina victima	Ejecución de malware en maquinas de usuarios que son el objetivo					x								x
	Acceso remoto a través de troyano o puerta trasera en el sistema de la victima	Programa malicioso						x							
	Instalar Malware	Ejecución de malware en maquinas de usuarios que son el objetivo				x			x		x				

Tabla 28. Riesgos de fase de instalación

1. Informe_Anual_PandaLabs_2017, 2. (Luh et al., 2017), 3.(Giura & Wang, 2013), 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Crowe, W, 2015), 9. (Al-Mohannadi, Mirza, Namanya et al.…, 2016), 10. (Christensen, 2013), 11. (Ioannou, Louvieris, Clewley, & Powell, n.d.), 12. (Bodeau & Graubart, 2013), 13. (Lockheed, 2014).

Los riesgos más resaltados en esta fase son escalar privilegios, ejecución de malware en máquina, instalación y ejecución de programas en segundo plano.

-Comando y Control

Fases	Riesgos mencionados por autor	Riesgos homologados	Autores											
			1	2	3	4	5	6	7	8	9	10	11	12	13
Comando y Control	Tener acceso a la información buscada	Robo de información	x												
	Botnets, DDOS	Red Infectada								x					
	Trojans	Malware								x					
	Alterar registros del sistema	Limpiar las huellas del ataque							x						
	Rootkits	Malware							x						
	Los intrusos tienen acceso a comando y control y las manos en el teclado acceso dentro del entorno objetivo	Control remoto de máquinas infectadas						x		x					
	Ejecución de malware manual para escalar privilegios y tener control	Ejecución de malware en maquinas de usuarios que son el objetivo						x					x		
	Mover datos sensibles	Robo de información			x										
	Encriptar datos	Usar Canales ocultos para extraer información (Ransomware)			x										
	Comprimir datos	Usar Canales ocultos para extraer información (Ransomware)			x										
	Acceso a información sensible	Robo de información			x										
	Control remoto de la maquina infectada	Control remoto de máquinas infectadas		x											x
	Comunicaciones ilegitimas por HTTP o HTTP	Establecer conexiones externas					x								
	Servidor que controla a la victima desde Internet y establece un canal C2	Establecer conexiones externas						x							
	Escalar privilegios de acceso	Escalar privilegios				x							x		
	Usuarios redirigidos a un sitio que aloja una carga maliciosa que establece puerta trasera	Backdoor					x								
	Backdoor que comunica con otro equipo	Backdoor					x								
	Navegación de base de datos, sistema de archivos y bases de datos	Escalar privilegios											x		
	Establece los canales de comunicación para acceder a los activos internos de la victima	Control remoto de máquinas infectadas	x		x					x	x				x

Tabla 29. Riesgos de la fase comando y control

1. Informe_Anual_PandaLabs_2017, 2. (Luh et al., 2017), 3.(Giura & Wang, 2013), 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Crowe, W, 2015), 9. (Al-Mohannadi, Mirza, Namanya et al.…, 2016), 10. (Christensen, 2013), 11. (Ioannou, Louvieris, Clewley, & Powell, n.d.), 12. (Bodeau & Graubart, 2013), 13. (Lockheed, 2014).

Los riesgos más resaltados en esta fase son escalar privilegios, ejecución de malware en máquina y control remoto de máquina infectada.

-Acción sobre los Objetivos

Fases	Riesgos mencionados por autor	Riesgos homologados	Autores											
			1	2	3	4	5	6	7	8	9	10	11	12	13
Acción sobre los Objetivos	Mantener conexón y persistencia silenciosamente por mucho tiempo	Control remoto de máquinas infectadas												x	
	Iniciar conexión externa	Establecer conexiones externas			x		x								
	Comprometer sistemas adicionales y moverse latera	Escalar privilegios													x
	Tranferir información a servidores externos	Robo de información			x		x								
	Exfiltración de datos sensibles	Robo de información		x								x			x
	Canal encubierto	Control remoto de máquinas infectadas				x									
	Perdida de integridad de datos	Perdida de integridad de los datos										x			x
	Borras Huellas de actividades maliciosas	Eliminar rastros y huellas post explotation		x										x	
	Lograr accesos a aplicaciones, información especificas o seguir moviéndose dentro de la red para buscar otros objetivos	Escalar privilegios	x							x	x				x
	Alterar Fechas de Archivo	Perdida de integridad de los datos							x						
	Daño físico / Robo / pérdida	Robo de información								x					x
	Cargue datos usando canales encubiertos encriptados a medios de almacenamiento externo o una nube	Robo de información											x		
	Divulgación de datos que implica recopilar, encriptar y extraer información del entorno de la victima	Perdida de integridad de los datos						x							x

Tabla 30. Riesgos presentes en fase acción sobre objetivos

Fuente de elaboración propia

Los riesgos más resaltados en esta fase perdida de integridad de los datos, escalar privilegios, robo de información.

En resumen los riesgos en cada de las fases del ciclo de vida de APT se muestra en la ilustración 5.

Ilustración 5. Resumen Riesgos más citados por fase.

Fuente de elaboración propia

3.2.2.Definición de políticas y buenas prácticas del framework

Después de identificar las fases del ciclo de vida y cómo opera un hacker a través de cada una de las fases para lograr el cometido, se comienzan a definir las políticas y buenas prácticas que conformaran el framework. En las siguientes ilustraciones se pueden apreciar al igual que en el anexo B, la forma como se obtuvieron. Estas buenas pràcticas han sido asociadas mas adelante para mitigar cadas riesgo que pueden presentar los activos del sector hospitalario.

Ilustración 6 Salvaguardas Fisicas

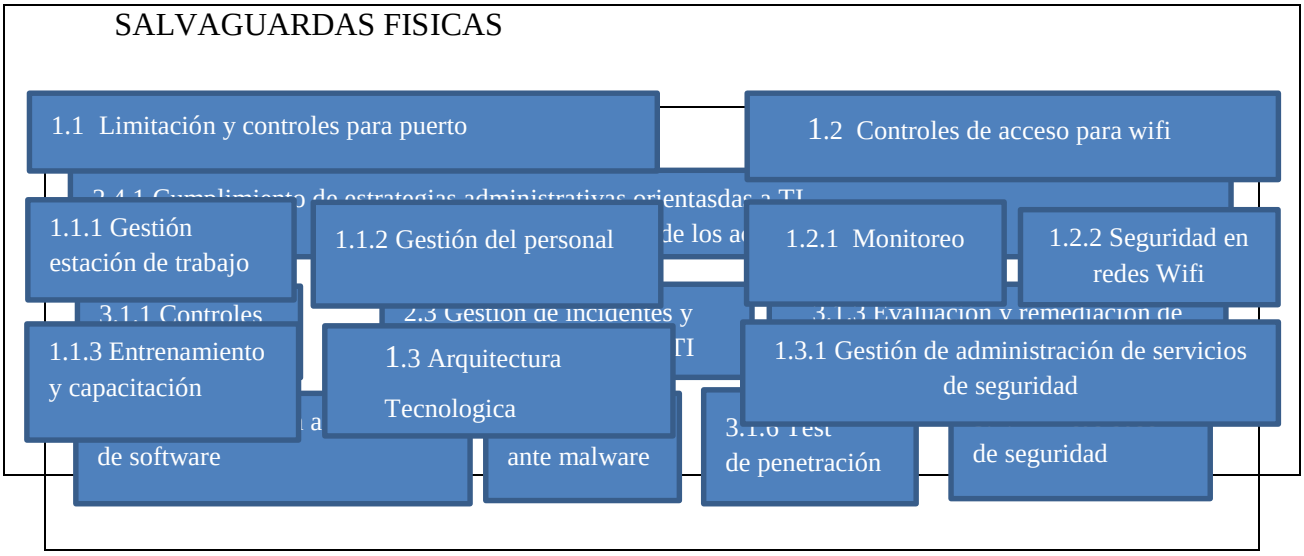


Ilustración 7 Salvaguardas técnicas

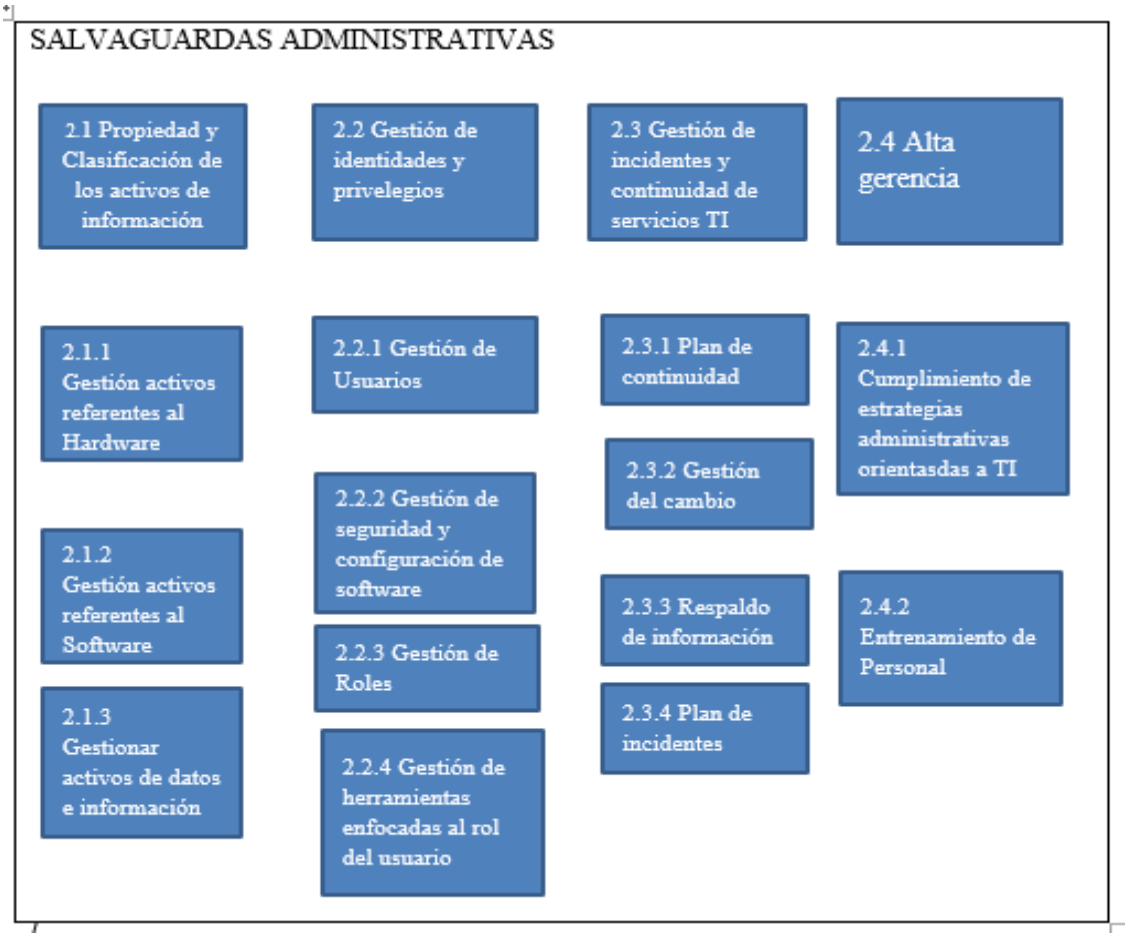


Ilustración 8 Salvaguardas Administrativas
Fuente de elaboración propia

3.2.3.Definición de controles asociados a los riesgos y a la fase del APT

Los controles que fueron homologados según las buenas prácticas de varios framework son el insumo principal para identificar cuáles de ellos pueden ser aplicados en cada una de las fases del ciclo de vida de acuerdo a los riesgos más vulnerables en cada una de las etapas, en las tablas 32 a 43 se hace referencia a los riesgos más importantes de cada una de las fases del ciclo de vida; en la parte superior de la tabla se encuentra el riesgo y dentro de este los controles homologados según las buenas prácticas que fueron recopiladas(las tablas que se verán a continuación son fuente de elaboración propia).

- **Contoles Fase de Reconocimiento**

Ingeniería Social	**Footprinting**
1.1.2 Gestión de personal 1.1.3 Entrenamiento y capacitación 1.2.1 Monitoreo 1.2.2 Seguridad en redes WIFI 2.2.2 Gestión y seguridad y configuración en software 2.4.2 Entrenamiento de personal 2.2.1 Gestión de usuarios 2.2.3 Gestión de roles 3.1.1 Control Criptográfico 3.1.4 Seguridad en aplicaciones de software. 3.1.7 Líneas base de seguridad.	1.1.3 Entrenamiento y capacitación 1.2.1 Monitoreo 1.2.2 Seguridad en redes WIFI 2.1.2 Gestión de activos referentes al software 2.2.2 Gestión y seguridad y configuración de software. 2.4.2 Entrenamiento de personal 3.1.1 Controles criptográficos

Tabla 31Controles fase de reconocimiento

Escaneo de Vulnerabilidades
1.1.3 Entrenamiento y capacitación 1.2.1 Monitoreo 2.3.4 Plan de incidentes 2.3.1 Plan de continuidad 2.4.2 Entrenamiento de personal 3.1.7 Líneas base de seguridad

Tabla 32. Controles para el riesgo de escaneo de vulnerabilidades

- **Controles fase Militarización**

Vulnerabilidades del día cero	Malware y Backdoor
2.2.1 Gestión de roles 2.2.2 Gestión de seguridad y configuración de software. 2.2.4 Gestión de herramientas enfocadas al rol del usuario 2.4.2 Entrenamiento de personal. 3.1.2 Mantenimiento, análisis y auditoria de logs 3.1.4 Seguridad en aplicaciones de software	1.1.1 Gestión estación de trabajo 1.2.1 Monitoreo 2.2.3 Gestión de roles 2.3.3 Respaldo de información 2.3.1 Plan de continuidad 2.3.4 Plan de incidentes. 2.4.1 Cumplimiento de estrategias administrativas orientadas a TI 2.4.2 Entrenamiento de personal 3.1.1 Controles criptográficos. 3.1.2 Mantenimiento, análisis y auditoria de logs. 3.1.3 Evaluación y remediación de vulnerabilidades 3.1.4 Seguridad en aplicaciones software 3.1.5 Defensa ante Malware

Tabla 33. Controles para los riesgos de la fase de militarización

Phishing	Herramientas maliciosas de entrega
1.1.1 Gestión estación de trabajo. 1.3.1 Gestión de administración de servicios de seguridad 1.1.1 Gestión de usuarios. 1.1.3 Gestión de roles 2.3.1 Plan de continuidad 2.4.2 Entrenamiento de personal 3.1.3 Evaluación y remediación de vulnerabilidades 1.1.7 Líneas base de seguridad.	1.1.1 Gestión de usuarios. 2.1.3 Gestionar activos de datos e información. 1.1.2 Gestión y seguridad y configuración del software. 1.1.3 Gestión de roles 2.2.4 Gestión de herramientas enfocadas al rol del usuario. 2.3.1 Plan de continuidad 2.3.4 Plan de incidentes 2.4.1 Estrategia para el cumplimiento de servicios administrativos 3.1.7 Líneas base de seguridad.

Tabla 34. Controles para el riesgo Phishing y uso de herramientas maliciosas

- **Controles fase Distribución**

Phishing
1.1.3 Gestión estación de trabajo. 1.3.1 Gestión de administración de servicios de seguridad 1.1.7 Gestión de usuarios. 1.1.8 Gestión de roles 2.3.1 Plan de continuidad 2.4.2 Entrenamiento de personal 3.1.3 Evaluación y remediación de vulnerabilidades Líneas base de seguridad

Phishing	**Sitios maliciosos**
1.1.2 Gestión estación de trabajo. 1.3.1 Gestión de administración de servicios de seguridad 1.1.4 Gestión de usuarios. 1.1.5 Gestión de roles 2.3.1 Plan de continuidad 2.4.2 Entrenamiento de personal 3.1.3 Evaluación y remediación de vulnerabilidades 1.1.6 Líneas base de seguridad.	1.1 Limitación y controles para puerto. 1.2 Controles para acceso wifi. 1.3. Alta gerencia 3.1 Seguridad en servicios de campo

Tabla 35. Controles para riesgos fase de distribución

- **Controles fase Explotación**

Vulnerabilidades conocidas	**Explotar equipos**
1.1.1 Gestión estación de trabajo 2.3.1 Plan de continuidad 2.3.2 Gestión del cambio 2.3.3 Respaldo de información 2.3.4 Plan de incidentes 2.4.2 Entrenamiento de personal 3.1.1 Controles Criptográficos. 3.1.2 Mantenimiento, análisis y auditoria de logs. 3.1.4 Seguridad en aplicaciones de software. 3.1.7 Líneas base de seguridad	1.1.1 Gestión estación de trabajo 1.1.2 Controles criptográficos 1.2.1 Monitoreo. 1.3.1 Gestión de administración de servicios de seguridad 2.2.2 Gestión y seguridad y configuración de software 2.2.3 Gestión de roles 2.3.1 Plan de continuidad 2.3.2 Gestión del cambio 2.3.3 Respaldo de información

	2.3.4 Plan de incidentes 2.4.2 Entrenamiento de personal 3.1.7 Líneas base de seguridad.

Tabla 36. Controles fase de explotación

- **Controles fase Instalación**

Escalar privilegios	**Ejecución de Malware**
1.1.1 Gestión estación de trabajo 1.2.1 Monitoreo 2.3.1 Plan de continuidad 2.3.2 Gestión de cambio 2.3.3 Respaldo para de información 2.3.4 Plan de incidentes 2.4.1 Cumplimiento de estrategias administrativas orientadas a TI. 2.4.2 Entrenamiento de personal 3.1.7 Líneas base de seguridad	2.2.1 Gestión del usuario 2.2.3 Gestión de roles 2.3.1 Plan de continuidad 2.3.2 Gestión del cambio 2.3.3 Respaldo de información 2.3.4 Plan de incidentes 2.4.2 Entrenamiento de personal 3.1.1 Controles criptográficos 3.1.4 Seguridad en aplicaciones software 3.1.5 Defensa ante Malware

Tabla 37. Controles fase de instalación

Recolección de credenciales de usuario	**Instalación y ejecución de programas en segundo plano**
1.1.4 Gestión estación de trabajo. 1.2.1 Monitoreo 1.3.1 Gestión de administración de servicios de seguridad 2.3.3 Respaldo de información 1.1.9 Gestión de usuarios. 1.1.10 Gestión de roles 2.3.1 Plan de continuidad 2.4.2 Entrenamiento de personal 3.1.3 Evaluación y remediación de vulnerabilidades 3.1.7 Líneas base de seguridad.	2.2.1 Gestión de usuarios. 2.2.3 Gestión de roles 2.1.3 Gestionar activos de datos e información. 2.2.2 Gestión y seguridad y configuración del software. 2.2.31.1.3 Gestión de roles 2.2.4 Gestión de herramientas enfocadas al rol del usuario. 2.3.1 Plan de continuidad 2.3.4 Plan de incidentes 2.4.1 Estrategia para el cumplimiento de servicios administrativos 3.1.7 Líneas base de seguridad.

Tabla 38. Controles fase instalación parte 2

- **Controles fase Comando y control**

Control Remoto de máquinas infectadas	Ejecución de malware
1.1.2 Gestión estación de trabajo 1.2.1 Monitoreo 2.2.3 Gestión de roles 2.3.3 Respaldo de información 2.3.1 Plan de continuidad 2.3.4 Plan de incidentes. 2.4.1 Cumplimiento de estrategias administrativas orientadas a TI 2.4.2 Entrenamiento de personal 3.1.1 Controles criptográficos. 3.1.2 Mantenimiento, análisis y auditoria de logs. 3.1.3 Evaluación y remediación de vulnerabilidades 3.1.4 Seguridad en aplicaciones software 3.1.5 Defensa ante Malware	2.2.1 Gestión del usuario 2.2.3 Gestión de roles 2.3.1 Plan de continuidad 2.3.2 Gestión del cambio 2.3.3 Respaldo de información 2.3.4 Plan de incidentes 2.4.2 Entrenamiento de personal 3.1.1 Controles criptográficos 3.1.4 Seguridad en aplicaciones software 3.1.5 Defensa ante Malware

Tabla 39. Controles fase de comando y control

- **Controles fase Acción sobre los objetivos**

Establecer conexiones externas	Escalar privilegios
1.3 Limitación y controles para puerto. 1.4 Controles para acceso wifi. 1.3. Alta gerencia 3.1 Seguridad en servicios de campo	1.1.2 Gestión estación de trabajo 1.2.1 Monitoreo 2.3.1 Plan de continuidad 2.3.2 Gestión de cambio 2.3.3 Respaldo para de información 2.3.4 Plan de incidentes 2.4.1 Cumplimiento de estrategias administrativas orientadas a TI. 2.4.2 Entrenamiento de personal 3.1.7 Líneas base de seguridad

Tabla 40. Controles fase de acción sobre los objetivos

Robo de información	Perdida de integridad de datos
1.1 Gestión estación de trabajo 1.2.1 Monitoreo 1.3.1 Gestión de administración de servicios de seguridad. 2.1.2 Gestión de activos referentes al software 2.1.3 Gestión de activos de datos e información. 2.2.1 Gestión de usuarios. 2.2.3 Gestión de Roles 2.2.4 Gestión de herramientas enfocadas al usuario. 2.3.1 Plan de continuidad. 2.3.3 Respaldo de información. 2.3.4 Plan de incidentes 2.4.2 Entrenamiento de personal 3.1.1 Controles criptográficos 3.1.6 Test de penetración. 3.1.3 Evaluación y remediación de vulnerabilidades 3.1.7 Línea base de seguridad.	2.1 Propiedad y clasificación de los activos de información. 2.3 Gestión de incidentes y continuidad de servicios de TI 3.1 Seguridad en servicios de campo.

Tabla 41. Controles fase de acción sobre los objetivos parte 2

Fuente de elaboración propia

3.2.4. Analis de resultados

Las buenas prácticas obtenidas a partir de diferentes framework permitieron identificar que hay muchas que comparten muchos de los conceptos importantes que debe tenerse para evitar la fuga de información.

Las buenas prácticas le permitirán a la organización hospitalaria que puede ser víctima de una amenaza persistente; mejorar la toma decisiones en cuanto a lo que tiene que ver con las inversiones tecnológicas que debes realizar.

Las buenas prácticas permitirán a la organización hospitalaria conocer de antemano los riesgos a los que la empresa se enfrenta acotando su impacto en la organización.

3.3. Herramientas para mitigar la fuga de información

Las siguientes herramientas son resultado de una rigurosa investigación de artículos científicos que trataban el modelo Kill Chain (Ver anexo C, ítem 6.3, tabla 74), y que fueron los que hicieron importantes aportes para poder clasificar un kit de herramientas que permitan al framework funcionar bajo el concepto de DLP. A continuación se muestra el resultado de este objetivo.

Herramientas según la fase del ciclo de vida del APT.

Fase de Reconocimiento:

Fase	Técnicas de prevención	Técnicas de detección	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Reconocimiento	Pruebas de seguridad , políticas de destrucción de documentos	Router Logs, Firewall logs			■					■			■	■	■		■
	Recopile registros de visitantes																
	Proteger la red para evitar el reconocimiento de servicios innecesarios	Políticas DROP para firewall															
	Actualizaciones	Antivirus															
	Registro de logs, http logs	Autenticación(Análisis de trafico DNS logs malicioso), Análisis de Malware		■	■		■	■		■	■	■	■				
	Contraseñas Seguras y cambio de contraseñas	controles de acceso lógico y físico										■				■	
	Educación en seguridad									■	■	■	■		■	■	■
	HIDS	NIDS		■		■			■	■							
	Filtrado de protocolos innecesarios.	Monitoreo de logs y de las conexiones TCP/UDP que se llevan a cabo en el servidor		■		■			■	■					■		
		Limitar la tasa de tráfico proveniente de un único host.		■		■			■	■					■		
	Prevenir inundaciones (floods) en los protocolos TCP/UDP	Limitar el número de conexiones concurrentes al servidor.		■		■			■	■							
		Restringir el uso del ancho de banda por aquellos hosts que cometan violaciones.		■		■			■	■							
	Análisis de navegador	Detección de firmas								■			■				■
	Evaluación de la vulnerabilidad utilizando un equipo azul y Rojo			■						■				■			
		Detección virtual de sambox		■						■				■			
		Máquinas de aprendizaje					■	■	■	■							
	Correlación de eventos, herramientas y técnicas de generación de gráficos de ataque	Análisis contextual(Enfoques Bayesianos), Análisis Web		■	■		■	■	■	■		■					
		Identificación basado en ataques de evasión	■														
	Segmentación de red, DMZ									■	■						
	Revisar la configuración de Routers y Firewalls	Caracterización de reputación (Listas Blancas, MET, SpamFlow)			■		■	■		■	■			■			
	ACL																

Tabla 42. Herramientas fase de reconocimiento

1. (Mustafa, 2013), 2. (Luh et al., 2017) , 3. (Giura & Wang, 2013) 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Moon, Im, Lee, & Park, 2014), 9. (Virvilis & Gritzalis, 2013), 10. (Crowe, W, 2015), 11. (Al-Mohannadi, Mirza, Namanya et al..., 2016), 12. (C h r i s t e n s e n, 2013), 13.(Ioannou, Louvieris, Clewley, & Powell, 2013)**, 14.**(Bodeau & Graubart, 2013)**, 15.**(Lockheed, 2014)

Fase Militarización

Fase	Técnicas de prevención	Técnicas de detección	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Militarización		Filtros de reputación (anti spam, antivirus ,Listas blancas,			■	■	■	■	■	■	■			■	■	■	■
	Recolecte archivos y metadatos para análisis futuros	Listas negras y listas de bloque en tiempo real basadas en DNS, ClamAV, SpamAssassin), filtro proxy, Detección de reglas, Políticas basadas en reglas.															
	Identificar e integrar las actividades de evaluación de controles de seguridad																
	Enumerar vulnerabilidades descubiertas																
	Analice la línea de tiempo de creación de malware	Análisis de artefactos de malware.															
	Determinar artefactos de armamento comunes a las campañas de APT																

Tabla 43. Herramientas fase de militarización

1. (Mustafa, 2013), 2. (Luh et al., 2017) , 3. (Giura & Wang, 2013) 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea et al., 2015), 6. (Hutchins et al., n.d.), 7. (Hutchins et al., n.d.), 8. (Moon et al., 2014), 9. (Virvilis & Gritzalis, 2013), 10. (Crowe, W, 2015), 11. (Al-Mohannadi, Mirza, Namanya et al..., 2016), 12. (C h r i s t e n s e n, 2013), 13.(Ioannou et al., 2013)**, 14.**(Bodeau & Graubart, 2013)**, 15.**(Lockheed, 2014)

Fase de Entrega

Fase	Técnicas de prevención	Técnicas de detección	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Entrega	Filtros de ejecución de contenido dinámico					■	■	■	■	■	■	■			■	■	
	NIPS	NIDS				■			■	■							
	Computación Segura y confiable basada en controles de software	Analice el medio de entrega									■	■				■	■
	Usuario vigilante								■								
	In-line AV					■			■			■			■		
	Queuing								■								
	Comprenda la infraestructura ascendente	Consumo de Recursos(para filtrar correo electrónico)			■	■	■	■			■	■				■	■
	Entender a los servidores y personas específicos, sus roles y responsabilidades	Random Forests Algorithm				■	■										■
	Recopile registros de correo electrónico y web para la reconstrucción forense	Dataset del email(Vortex-IDS, WEKA),				■	■				■						■
	Detectar nuevas cargas maliciosas en el punto de entrega	Herramientas de Clasificación de correos				■					■	■					■

Tabla 44.Herramientas fase de entrega

1. (Mustafa, 2013), 2. (Luh et al., 2017) , 3. (Giura & Wang, 2013) 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea et al., 2015), 6. (Hutchins et al., n.d.), 7. (Hutchins et al., n.d.), 8. (Moon et al., 2014), 9. (Virvilis & Gritzalis, 2013), 10. (Crowe, W, 2015), 11. (Al-Mohannadi, Mirza, Namanya et al..., 2016), 12. (C h r i s t e n s e n, 2013), 13.(Ioannou et al., 2013)**, 14.**(Bodeau & Graubart, 2013)**, 15.**(Lockheed, 2014)

Fase de Explotación

Fase	Técnicas de prevención	Técnicas de detección	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Explotación	Capacitación de usuarios	HIDS															
	Pruebas de correo electrónico para los empleados	Restringir privilegios de administrador															
	Actualizaciones(Patch), hardening, Corregir las Vulnerabilidades	Monitorear Alertas del sistema															
	DEP(Prevención de ejecución de datos de Windows)	Bloquear ejecución de programas sin autorización.															
	Capacitación de codificación segura para desarrolladores web	Auditoría del proceso del punto extremo para análisis forense y conocer origen del exploit															
	Análisis de vulnerabilidades y pruebas de penetración regulares-	Medidas de refuerzo del punto final- Reglas del punto final personalizado para bloquear la ejecución del código Shell															

Tabla 45.Herramientas fase de explotación

1. (Mustafa, 2013), 2. (Luh et al., 2017) , 3. (Giura & Wang, 2013) 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea et al., 2015), 6. (Hutchins et al., n.d.), 7. (Hutchins et al., n.d.), 8. (Moon et al., 2014), 9. (Virvilis & Gritzalis, 2013), 10. (Crowe, W, 2015), 11. (Al-Mohannadi, Mirza, Namanya et al..., 2016), 12. (Christensen, 2013), 13.(Ioannou et al., 2013)**, 14.**(Bodeau & Graubart, 2013)**, 15.**(Lockheed, 2014)

Fase de Instalación

Fase	Técnicas de prevención	Técnicas de detección	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Instalación	Restringir Privilegios	HIDS															
	Entender el malware	Auditoría de proceso de punto final															
		Extrae certificados de cualquier archivo ejecutable firmado															
	Chroot jail	Crear nuevas mitigaciones de punto final.															
	AV	HIPS															

Tabla 46. Herramientas fase de instalación

1. (Mustafa, 2013), 2. (Luh et al., 2017) , 3. (Giura & Wang, 2013) 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea et al., 2015), 6. (Hutchins et al., n.d.), 7. (Hutchins et al., n.d.), 8. (Moon et al., 2014), 9. (Virvilis & Gritzalis, 2013), 10. (Crowe, W, 2015), 11. (Al-Mohannadi, Mirza, Namanya et al..., 2016), 12. (Christensen, 2013), 13.(Ioannou et al., 2013)**, 14.**(Bodeau & Graubart, 2013)**, 15.**(Lockheed, 2014)

Fase mando y control

Fase	Técnicas de prevención	Técnicas de detección	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Mando y control	Firewall ACL	NIDS		■	■	■	■	■	■	■					■	■	■
	DLP	Bloqueando el canal C2	■												■		■
	Software para ocultar las pulsaciones de teclado	Análisis completo de malware en la infraestructura C2											■	■			■
	Usar un enfoque de las ErsatzPasswords para mejorar la seguridad de los hashes	Bloquear la categoría proxy, incluidos los dominios "ninguno" o "sin categoría".											■				■
	Cifrado de datos												■				■
	NIPS	Intoxicación del receptor de DNS y envenenamiento del servidor de nombres				■			■								■
	Tarpi	Red Harden							■						■		■
	DNS redirect	Llevar a cabo investigaciones de código abierto para descubrir nuevas infraestructuras C2 adversas			■	■	■	■	■								■
	Personalice bloques de protocolos C2 en proxies web																

Tabla 47.Herramientas fase de mando y control

1. (Mustafa, 2013), 2. (Luh et al., 2017) , 3. (Giura & Wang, 2013) 4. (Deshmukh, Shelar y Kulkarni, 2014), 5. (Oprea et al., 2015), 6. (Hutchins et al., n.d.), 7. (Hutchins et al., n.d.), 8. (Moon et al., 2014), 9. (Virvilis & Gritzalis, 2013), 10. (Crowe, W, 2015), 11. (Al-Mohannadi, Mirza, Namanya et al..., 2016), 12. (C h r i s t e n s e n, 2013), 13.(Ioannou et al., 2013)**, 14.**(Bodeau & Graubart, 2013)**, 15.**(Lockheed, 2014)

Acción sobre los objetivos

Fase	Técnicas de prevención	Técnicas de detección	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Acción sobre los objetivos	Quality of service(calidad del servicio)	Audit log		■	■	■			■						■	■	■
		Estrategias de respuesta ante incidentes															
		Plan de comunicaciones															
	Honeypot	Capturas de paquetes de red							■								■
		Realizar una evaluación de daños															
	Incluir las lecciones aprendidas	Entender el ataque (Análisis Forense en puntos finales)											■	■		■	■

Tabla 48.Herramientas fase de acción sobre los objetivos

3.3.1. Modo de selección del Kit de Herramientas Propuestas para framework

Para probar la efectividad de algunas herramientas se realizó la prueba de ellas en un ambiente controlado (montaje de un sistema operativo Windows 2008 con 3 GB de RAM y máquinas virtuales kali con 2 GB de RAM, donde se hizo la instalación de las herramientas anteriormente descritas y se procedió con las pruebas de efectividad). Además en algunos casos fue necesario usar maquinas reales para realizar pruebas, debido a que ciertas amenazas están diseñadas para evadir la virtualización. Para todo lo anterior dichas pruebas se propusuieron atributos que se muestran en el anexo C. Fue necesario diseñar una plantilla para probar la efectividad de las pruebas, donde se observan las fases del cilco de vida del APT para las cuales aplica dicha herramienta y se homologó efectividad mapeando la valoración que define la ASD (Dirección Australiana de Señales) y de autores internacionales citados en la tabla 55 a 61, los cuales realizaron pruebas anteriomente a la mayoría de herramientas propuestas.

A continuación se muestran los atributos que se tuvieron en cuenta en las pruebas (Ver Anexo C, ítem 6.3. Pruebas de herramientas):

Fases del Ciclo de Vida del APT (Kill Chain)

1	Reconocimientos
2	Militarización
3	Distribución
4	Explotación
5	Instalación
6	Comando y Control
7	Acción sobre los objetivos

Valoración De Efectividad De Herramientas (Homologado de rangos asignados en ASD)

Valor	Rango de Efectividad
1	Bajo
2	Medio
3	Alto
4	Excelente

Ejemplo de plantilla de pruebas

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes en el protocolo Web HTTPS.
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave o expresiones regulares.
	2. Escribir un mensaje que contenga información confidencial y enviarlo desde un correo electrónico WEB que utilice cifrado HTTPS.
	3. Verificar el correcto envió del correo electrónico.
	4. Verificar la correcta detención de los incidentes a través del reporte
Resultados esperados	1. Herramienta DLP reporta el incidente
	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola
Efectividad	Excelente

Tabla 49. Atributos para realizar las pruebas y clasificar las herramientas.
Fuente de elaboración propia

Como se mencionó anteriormente el ambiente controlado se hizo con máquinas que tienen instalado sistemas Windows cuyas características en el software instalado y hardware son similares a las que se manejan en la mayoría de los ambientes hospitalarios.

Las herramientas que se proponen han sido sacadas de la ASD (Dirección Australiana de Señales) y de las que proponen autores internacionales, según cada fase del ciclo de vida del APT citados en la tabla 55 a 61, con el fin de proporcionar estrategias de mitigación para el riesgo de seguridad que representan las APTs que usan el vector de ataque correos electrónicos. En la tabla 49 se muestra el resultado de la evaluación del kit de herramientas y que fueron clasificadas según la fase para las cuales aplica. Para ver pruebas remitase al anexo C.

A continuación se muestra la evaluación que surgio como resultado de las pruebas de las herramientas (Tabla 49, herramientas seleccionadas por su nivel de efectividad y según estudios de autores.Ver anexo C, ítem 6.3. Pruebas de herramientas, tabla 74).

Evaluación de Herramientas y Estratégicas para Prevenir ataques APT

Herramientas	Estrategia de mitigación	Efectividad (ver anexo B)	Prevenir o detectar una intrusión	Fases del ciclo de vida (Kill Chain) APT donde se puede utilizar						
				1	2	3	4	5	6	7
Filtro web	Convertir archivos adjuntos a otro tipo de archivo, listas blancas dinámicas, listas negras y listas de bloque en tiempo real basadas en DNS, Spam Assassin, configuración de reglas, políticas basadas en reglas.	Excelente	Prevenir		x	x			x	x
Filtro Proxy	Archivos adjuntos de lista blanca basados en la tipificación de archivos, bloquear archivos protegidos con contraseña, archivos adjuntos no identificados o encriptados	Excelente	Prevenir		x	x			x	x
Herramientas de análisis dinámico de malware	Realice un análisis dinámico automatizado de archivos adjuntos ejecutados en una caja de arena.	Excelente	Prevenir		x	x				x
		Excelente	Prevenir		x	x				
	Desinfecte los archivos adjuntos para eliminar contenido activo o potencialmente dañino	Excelente	Prevenir			x				
	Deshabilitar o controlar macros en archivos de Microsoft Office	Excelente	Prevenir			x				
Anti-Malware	Inspección controlada de archivos archivados Inspección de archivos de Microsoft Office en estaciones de trabajo Usar una solución antivirus en base a firmas	Medio	Ambos			x				x
	Archivos adjuntos de listas negras basados en la escritura de archivos	Alto	Prevenir			x				

	Escanear archivos adjuntos utilizando software antivirus	Bajo	Prevenir			x				
	Archivos adjuntos de listas negras basados en la extensión de archivo	Bajo	Ambos			x				x
Herramientas anti-spam	Probrar mediantes test el nivel de seguridad anti- spam, reemplace las direcciones web activas dentro del cuerpo de un correo electrónico con versiones no activas	Medio	Prevenir		x	x				
	Eliminar contenido activo del cuerpo de un correo electrónico	Alto	Prevenir			x				
Herramienta de Filtrado de correo electrónico	Implementar DMARC (Autenticación de mensajes, informes y conformidad basada en dominios) para mejorar SPF(Convenio de Remitentes, del inglés Sender Policy Framework) y / o DKIM(Domain Keys Identified Mail)	Medio	Prevenir			x				
	Bloquear el correo electrónico en SenderID / SPF 'hard failure'	Alto	Prevenir			x				
	El correo electrónico bloqueado en DKIM fail	Alto	Prevenir			x				
	Incorporar listas negras de spam	Medio	Ambos			x				x
	Poner en cuarentena el correo electrónico en SenderID / SPF 'soft fail'	Medio	Prevenir			x				
Herramientas para test de Seguridad e intrusión y exploración de redes	Realizar pruebas de seguridad a los sistemas y empleados	Superior	Prevenir	x		x	x			
Herramientas de análisis de logs(router	Analizar los registros de los eventos sospechosos del router	Alto	Identificar	x		x	x			
	Analizar los registros de los eventos sospechosos del firewall	Alto	Identificar	x		x	x			

logs, Firewall logs, http logs)	Analizar los registros de navegación y visitas de usuarios en las aplicaciones web	Alto	Identificar	x		x	x			
Herramienta de análisis de trafico DNS logs malicioso	Realizar Análisis de DNS logs maliciosos pueden ayudar en la predicción del grado de legitimidad de un dominio.	Excelente		x		x	x			
Herramientas de evaluación de la vulnerabilidad	Descubrir vulnerabilidades de los sistemas	Alto		x	x					
Herramientas de gestión de parches	Parchar vulnerabilidades en las aplicaciones	Alto	Ambos	x			x			
	Parchar vulnerabilidades en el sistema operativo			x			x			
Web Control (bloqueo de scripts en navegadores web), Web Anti-Virus	Endurecimiento de la configuración de las aplicaciones del usuario	Alto	Prevenir	x			x			
Mail Anti-Virus y Web Anti-Virus, Security for Mail Server, Security for Internet Gateway, ClamAV, Anti-Spam	Análisis dinámico automatizado de correo electrónico y contenidos web Filtrado de contenidos de correo Listas blancas de dominios web Bloqueo de mensajes de correo fraudulentos Solución antivirus en base al método heurístico y clasificaciones automáticas de reputación en Internet	Alto	Ambos		x	x		x		

DLP for Mail y Collaboration add-ons	Aplicar políticas, listas blancas de dominio web, configurar agentes, bloqueo de mensajes de correo fraudulentos, bloqueo de dispositivos, evitar fuga de información que abarca las realidades de hoy en día centradas en la nube y en la movilidad con DLP.	Excelente	Ambos		x	x		x	x	
Herramienta Data Execution Prevention (DEP)	Realizar comprobaciones adicionales en la memoria para ayudar a evitar que código malicioso se ejecute en un sistema	Excelente	Prevenir			x	x	x		
Herramientas para prevención automática de exploits, Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Mitigación de vulneraciones genéricas del sistema operativo	Excelente	Prevenir			x	x	x		
HIDS / HIPS, NIDS	Incluir los sistemas de monitoreo y aplicaciones de control de privilegios	Superior	Ambos				x	x	x	
Advanced Firewall	Cortafuegos de aplicaciones basadas en software para el tráfico de entrada y salida	Superior	Prevenir						x	
Herramienta de analítica de seguridad	Registro de sucesos del ordenador y actividades de la red	Alto		x		x	x			
Herramientas para device control	Control de medios removibles y portátiles	Alto		x						

Sistemas de autenticación	Control de accesos de usuarios	Alto		x		x	x			
Herramientas para aplicación de servidores que refuercen las aplicaciones web accesibles a Internet y bases de datos(Usar certificado TLS)	Desinfecte las entradas y use TLS no SSL, proteja las bases de datos, así como las aplicaciones que acceden a datos importantes (confidenciales / de alta disponibilidad).	Alto	Prevenir	x				x		
Herramientas de monitoreo de logs y conexiones TCP/UDP	Hacer monitoreo de los registros de los eventos sospechosos del router.	Superior	Detectar			x	x			x
Herramientas VPN, RDP, SSH	Autenticación de múltiples factores para todos los usuarios que realizan acciones privilegiadas o acceden a recursos(sensible o de alta disponibilidad)	Superior	Prevenir	x		x	x			
Herramientas Virtual Sandbox, Maquinas de Aprendizaje	Entorno de espacio aislado virtualizado no persistente, para denegar el acceso a datos importantes en actividades riesgosas, exploración web y visualización de archivos de procedencia sospechosa.	Alto	Prevenir	x		x				
Herramienta Honeypot	Simular una red local de múltiples equipos, ips falsas, directorios inventados, equipos no presentes para crear confusión al atacante. También se usa para detectar nuevos métodos de ataque y poder responder a esas amenazas en la red real	Alto	Ambos							x
Herramientas de Auditoria de logs	Análisis forense de procesos y punto final	Alto	Detectar					x		x

Herramienta para Chroot Jail	Limitar las capacidades de las maquinas en gran medida mediante una cárcel chroot y evitar que los usuarios no accedan a otros recursos no autorizados.	Alto	Prevenir					x		
Herramienta para validar certificados de archivos ejecutables	Implementar un validador de los certificados de los archivos ejecutables para evitar ser infectado.	Alto	Ambos			x		x		

Tabla 50. Herramientas seleccionadas según su efectividad.

La tabla 67 sirve como insumo para identificar las fases en las que pueden ser usada las herramientas de mitigación y poder valorar la efectividad de ellas. Son de insumo al framework a la hora de hacer uso de las buenas prácticas y herramientas que se encuentran en la tabla 68, donde se muestra la estrategia con su respectiva fase para la cual fue creada.

3.3.2. Análisis de resultados

Se logró comprobar la efectividad de las herramientas que los autores y los organismos internacionales recomiendan, muchas tienen mucha flexibilidad para la creación de reglas, ya que mediante la utilización de ciertos parámetros es posible personalizar las reglas para poder detectar tráfico malicioso y se identificó que los sistemas DLP, IDS e IPS ayudan a monitorear los dispositivos y el tráfico malicioso de la red y hacer frente a ataques conocidos, sin embargo si no hay reglas configuradas para ataques desconocidos, la capacidad de detección es casi nula.

Los sistemas DLP están diseñados para evitar fuga de información y demostraron ser efectivos a la hora de bloquear cualquier intento de extracción de información, pero si no existen los políticas claras para los empleados será casi que imposible hacerlo, por esta razón el framework que se propuso permite tener buenas prácticas y herramientas integrales para evitar tener áreas aisladas.

Se pudo apreciar en la práctica que para maximizar la efectividad de las herramientas se deben incorporar buenas configuraciones y actualizaciones a este tipo de sistemas, lo que genera un gran problema si no se configuran bien, debido a que se pueden crear falsos positivos y de esta manera será imposible responder a las amenazas latentes.

Se puede evidenciar que las herramientas IDS, proxy, IPS, firewall y entre otras herramientas le permite a los administradores de redes conocer cuando sus redes están siendo atacadas y permite conocer variables importantes para identificar los tipos de ataque, así mismo permite saber cuál puede ser el origen y causa.

Es posible mediante un sistema de prevención de intrusos detener ataques de amplificación o de cualquier tipo, haciendo uso de la configuración de reglas IPS y configurando reglas de firewall para poder filtrar todo el tráfico entrante y saliente.
Mediante el escaneo de vulnerabilidades en los equipos permite conocer los servicios y puertos innecesarios y las actualizaciones evitan que los atacantes ingresen con facilidad a los sistemas.

3.4. Construcción del framework.

Esta sección tiene como objeto mostrar la interacción del conjunto de artefactos y elementos que componen el framework de seguridad informática para mitigar la detección de APT. Para lo cual se unifican los resultados obtenidos en el ítem 3.1. "Guía de identificación de activos", 3.2. Buenas prácticas y 3.3. Herramientas para mitigar la fuga de información. To lo anterior sirven como insumo para identificar, detectar y proponer un conjunto de buenas prácticas y herramientas, teniendo en cuenta las fases del ciclo de vida de las APT y según sus riesgos.

El framework de seguridad informática está compuesto por la guía de identificación de activos sensibles a fuga de información para mitigar las APT, teniendo en cuenta los controles propuestos en las buenas prácticas y herramientas según las fases del ciclo de vida del APT(ver ítem 3.1, 3.2 y 3.3). Así mismo permite identificar los riesgos a los que puede estar expuesto el activo (ver ítem 3.2.1, Riesgos presentes en cada fase). Las herramientas que se proponen deben seguirse teniendo en cuenta la fase en la que se debe usar, estás pueden ayudar a mitigar e identificar los posibles riesgos de ser atacado, como también realizar una rigurosa investigación de un suceso mal intencionado para encontrar los responsables o entender el funcionamiento del ataque.

3.4.1. Framework de Seguridad informática

El framework está compuesto de los elementos que se aprecian en la ilustración 9, donde se aprecia las entradas y salidas del framework:

Para valorar sus activos informáticos en el sector salud el framework propone los siguientes pasos.

I. Identificar los activos sensibles a fuga de información mediante la guía de identificación de activos propuesta en el capítulo 2. Seguir guía para realización de este proceso.

II. Identificar los Riesgos asociados a las amenazas de los activos que fueron clasificados en la fase de activos vs amenazas que son susceptibles a fuga de información, de acuerdo a nivel de clasificación que determina dicho atributo. Ver ilustración 10.

A continuación se muestra el proceso que el administrador de sistemas (actor) sigue el framework para que sea entendible y pueda llevar a cabo dicho procedimiento en la entidad hospitalaria.

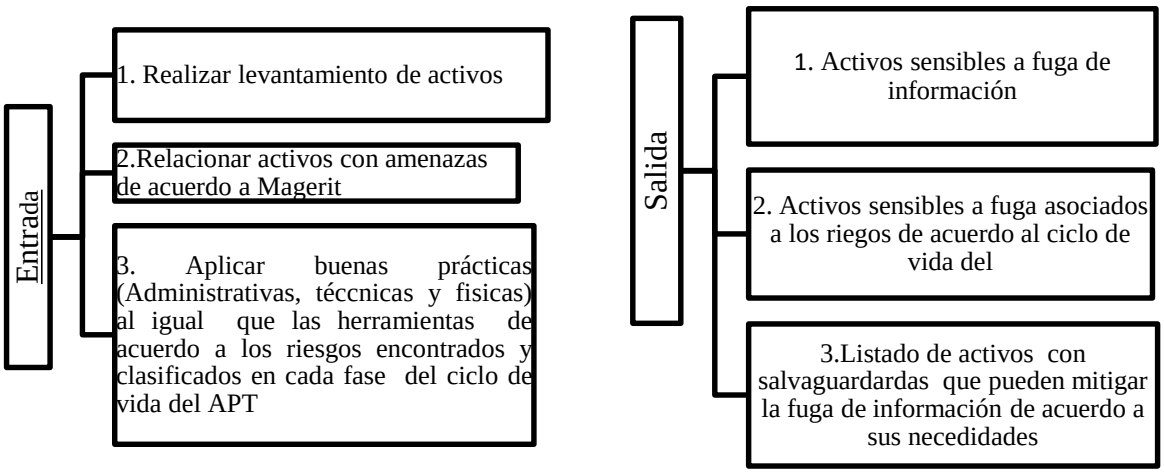


Ilustración 9. Framework de seguridad informática sector salud Fuente de elaboración propia.

3.4.2.Aplicabilidad del Framework

Para el proceso anteriormente mencionado se debe tener la lista de activos sensibles a fuga de información obtenidos en la guía de identificación (Ver ítem 3.1), para la cual se tiene que realizar el filtro correspondiente de dichos activos que se necesita proteger. Los cuáles serán tomados como entradas del framework. Para el cual se deben ingresar en el siguiente formato que se muestra en el ítem 3.1.5.5, tabla 58 y aplicar los controles y herramientas seleccionando la fase a la cual pertenece cada uno de ellos, tenga en cuenta los riesgos asociados y haga el comparativo de riesgos de los activos versus riesgos de buenas prácticas, los cuales denominaremos controles seguir el paso a paso del framework de acuerdo a la ilustración 10:

Riesgos asociados a cada amenaza que se identificó en la guía.

Riesgos	Fase	Amenazas
Escalar privilegios	Instalación-Acción sobre los objetivos	AP
Ejecución de malware	Instalación-Comando y Control	AP
Instalación y ejecución de programas en segundo plano	Instalación	AP
Control remoto de maquinas infectadas	Comando y Control	AP
Establecer conexión externas	Acción sobre los objetivos	AP
Footprinting	Reconocimiento	EA
Escaneo de vulnerabilidades	Reconocimiento	EA
Malware	Militarización	EA
Backdoor	Militarización	EA
Dispositivos infectados.	Distribución	EA
Recoleccion de credenciales de usuario.	Instalación	EA
Vulnerabilidades del dia cero	Militarización- Explotación	ERE
Explotación de equipos	Explotación	ERE
Ingenieria social	Reconocimiento	ES
Phishing	Militarización-Distribución	ES
Sitios maliciosos	Distribución	ES
Robo de información	Acción sobre los objetivos	FI
Pérdida de integridad de datos	Acción sobre los objetivos	INE
Herramientas maliciosas de entrega	Militarización	SI

Ilustración 10.Riesgos asociados a cada amenaza

Tabla con las amenazas según la modelación realizada en el objetivo 1.

Leyendas			
[EA]	Errores de Administrador	[SI]	Suplantacion de identidad
[ERE]	Errores de Reencademamiento	[AP]	Usuarios Privelegiados
[FI]	Fuga de Informacion	[INE]	Interceptacion de información
		[ES]	Ingenieria Social

Tabla 51. Amenazas de la guía de identificación de activos

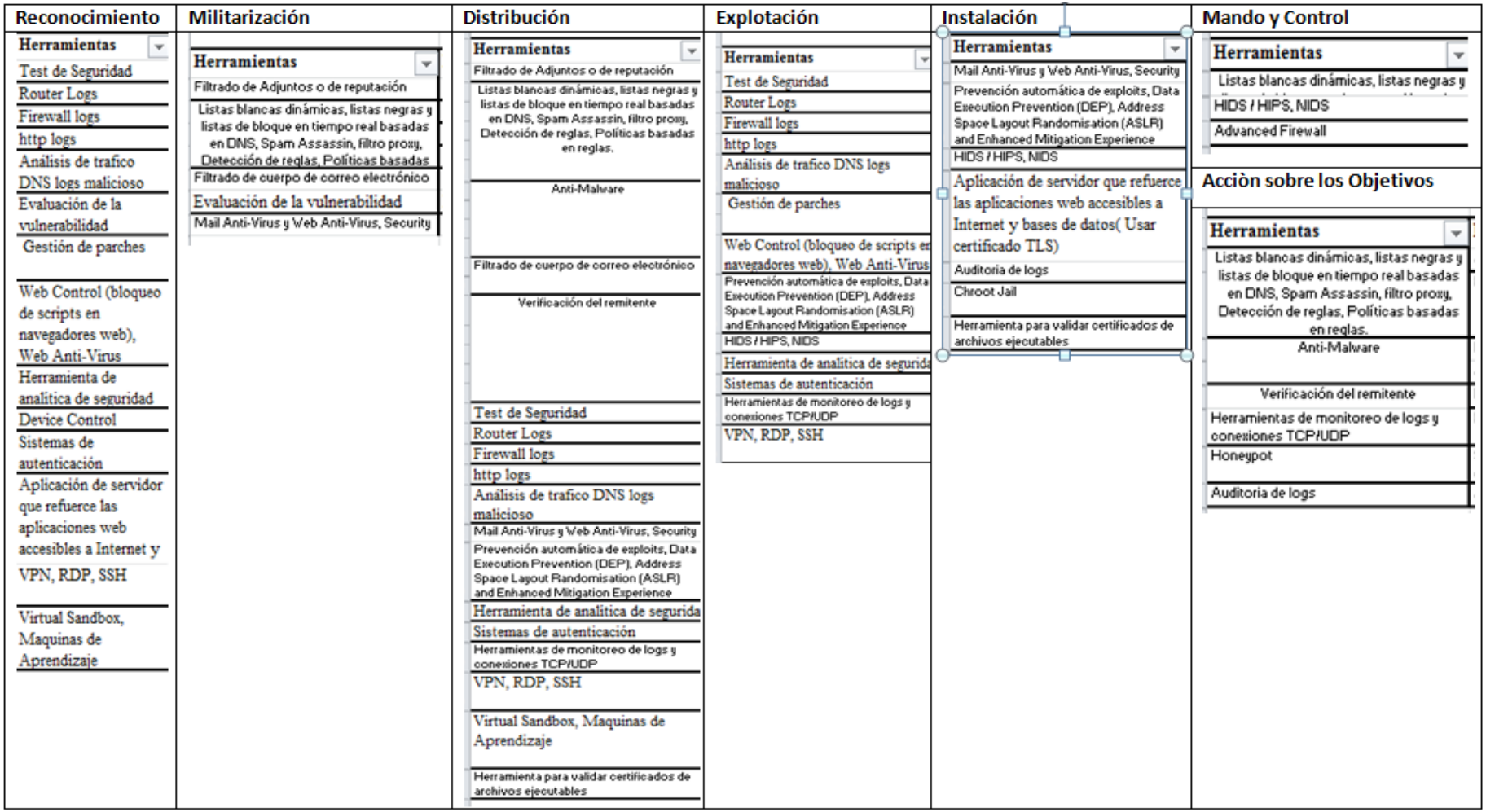
Se propone buenas prácticas(Ver ítem 3.2) y herramientas (Ver Item 3.3) para mitigar cada uno de los riesgos que fueron detectados con la guía propuesta como resultado del objetivo 2. En el resultado del objetivo 3 se proponen una serie de estratégias y herramientas por cada riesgo asociados a cada fase del ciclo de vida del APT. Ver tablas 41 a 47 y tabla 51 (herramientas para su aplicación según sea el riesgo asociado al activo y la fase en la que se puede usar).

Recuerde que es necesario tomar estrategias de mitigación con herramientas tecnológicas las cuales pueden servir como un procedimiento estándar a la hora de defenderse antes de un ataque o al momento de ser atacado.

Aplique las herramientas que se proponen, teniendo en cuenta los riesgos encontrados según la fase crítica asociada al riesgo, recordar que estas herramientas son las que según los autores que usan el Modelo de Kill Chain, pueden ayudar a mitigar las amenazas a las que están expuestos los activos de acuerdo a la fase del ciclo de vida del APT.

A continuación se muestra un resumen de las herramientas del framework que un administrador del área de sistemas de la entidad hospitalaria puede tomar como referencia.

Tabla 52. Herramientas del framework



Reconocimiento	Militarización	Distribución	Explotación	Instalación	Mando y Control
Herramientas	**Herramientas**	**Herramientas**	**Herramientas**	**Herramientas**	**Herramientas**
Test de Seguridad	Filtrado de Adjuntos o de reputación	Filtrado de Adjuntos o de reputación	Test de Seguridad	Mail Anti-Virus y Web Anti-Virus, Security	Listas blancas dinámicas, listas negras y
Router Logs	Listas blancas dinámicas, listas negras y listas de bloque en tiempo real basadas en DNS, Spam Assassin, filtro proxy, Detección de reglas, Políticas basadas	Listas blancas dinámicas, listas negras y listas de bloque en tiempo real basadas en DNS, Spam Assassin, filtro proxy, Detección de reglas, Políticas basadas en reglas.	Router Logs	Prevención automática de exploits, Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience	HIDS / HIPS, NIDS
Firewall logs	Filtrado de cuerpo de correo electrónico	Anti-Malware	Firewall logs	HIDS / HIPS, NIDS	Advanced Firewall
http logs	Evaluación de la vulnerabilidad	Filtrado de cuerpo de correo electrónico	http logs	Aplicación de servidor que refuerce las aplicaciones web accesibles a Internet y bases de datos(Usar certificado TLS)	**Acciòn sobre los Objetivos**
Análisis de trafico DNS logs malicioso	Mail Anti-Virus y Web Anti-Virus, Security	Verificación del remitente	Análisis de trafico DNS logs malicioso	Auditoria de logs	**Herramientas**
Evaluación de la vulnerabilidad		Test de Seguridad	Gestión de parches	Chroot Jail	Listas blancas dinámicas, listas negras y listas de bloque en tiempo real basadas en DNS, Spam Assassin, filtro proxy, Detección de reglas, Políticas basadas en reglas.
Gestión de parches		Router Logs	Web Control (bloqueo de scripts en navegadores web), Web Anti-Virus	Herramienta para validar certificados de archivos ejecutables	Anti-Malware
Web Control (bloqueo de scripts en navegadores web), Web Anti-Virus		Firewall logs	Prevención automática de exploits, Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience		Verificación del remitente
Herramienta de analitica de seguridad		http logs	HIDS / HIPS, NIDS		Herramientas de monitoreo de logs y conexiones TCP/UDP
Device Control		Análisis de trafico DNS logs malicioso	Herramienta de analitica de seguridad		Honeypot
Sistemas de autenticación		Mail Anti-Virus y Web Anti-Virus, Security	Sistemas de autenticación		Auditoria de logs
Aplicación de servidor que refuerce las aplicaciones web accesibles a Internet y		Prevención automática de exploits, Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience	Herramientas de monitoreo de logs y conexiones TCP/UDP		
VPN, RDP, SSH		Herramienta de analitica de seguridad	VPN, RDP, SSH		
Virtual Sandbox, Maquinas de Aprendizaje		Sistemas de autenticación			
		Herramientas de monitoreo de logs y conexiones TCP/UDP			
		VPN, RDP, SSH			
		Virtual Sandbox, Maquinas de Aprendizaje			
		Herramienta para validar certificados de archivos ejecutables			

Fuente de elaboración propia

3.4.3. Artefactos del framework

A continuación, se muestra un ejemplo de la salida que arrojó la guía que se propuso en objetivo 1 y sirve como artefacto del framework (ver anexo A, ítem 6.1). Estos sirven como insumo del framework para identificar los controles y buenas prácticas para los activos sensibles a fuga de información. Solo se deben tener en cuenta los activos cuya calificación es media, alta y superior.

Ejemplo de Lista de Activos clasificados con la guía propuesta

Codigo_a	Nombre Activo	Codigo_Impacto	Sensibilidad_activo	Nivel_fuga	Calificación
7	Analizador de Quimica Clinica SELECTRA PROS Con modulo ISE	1	0,6	0,6	INFERIOR
8	Analizador de Orina H500 DIRUI	0	0,6	0,6	INFERIOR
9	Analizador de Hematologia	0	0,6	0,6	INFERIOR
10	Analizador Quimica A-15 S/N 831051483	0	0,6	0,6	INFERIOR
11	Centrifuga de 24 Tubos C/Tacometro Digital	0	0,6	0,6	INFERIOR
12	Omax 40x X Microscopio Binocular Compuesto De Laboratorio C	0	0,6	0,6	INFERIOR
13	Microcentrifuga ref. CT-1D	0	0,6	0,6	INFERIOR
14	Agitador de mazzini V Variable 803621	0	0,6	0,6	INFERIOR
15	Cuenta globulos ref. CG 97, Equipo Electronico digital	0	0,6	0,6	INFERIOR
16	Centrifuga 12 tubos CIENTIFIC	0	0,6	0,6	INFERIOR
17	Centrifuga 12 tubos CIENTIFIC	0	0,6	0,6	INFERIOR
20	Autoclave AUTOMAT 3000 S/3000-0692	0	0,6	0,6	INFERIOR
27	Ecografo EDAN DUS3 con transductor convexo s/317206-M13101620001	0	0,6	0,6	INFERIOR
28	Electrocardiografo EDAN SE-3 S/SE3B323113140611,	0	0,6	0,6	INFERIOR
29	Equipo de rayos x ELITY 70 S/0234, con negatoscopio	1	0,6	0,6	INFERIOR
30	Equipo de Escritorio SO. 8.1 pro	2	2	6	MEDIO
31	Equipo de Escritorio SO. 8.1 pro	2	2	6	MEDIO
32	Equipo Compaq 18 windows 8.1 Pro	2	2	6	MEDIO
33	Sony PAI_MONDOMO-PC windows 7 professional	2	1,3	5,3	MEDIO
34	PC Sion Windows 7 ultimate	2	2	6	MEDIO
35	PC Sion MonCons3 Windows 8.1 pro, Microsoft office 2013	2	2	6	MEDIO
36	PC FACTURACIÃ"NMOND Windows xp, Microsoft Office 2007	2	2	6	MEDIO
37	PC Compumax FACTURACION CENTRO windows 2007, Microsoft office 2007	2	2	6	MEDIO
38	PC Lenovo- Windows 8.1 single language Microsoft office 2010	2	2	4	BAJO
39	Pc- SAMSUNG- Contabilidad- Windows 2007 Microsoft office 2003	2	2	6	MEDIO
40	Pc-Contratacion -windows 7 ultimate microsoft office 2010	2	2	6	MEDIO
41	Pc- Citologia- windows 8,1 pro microsoft Office 2010	2	2,7	6,7	MEDIO
42	Pc -sistemas2 -windows 10 microsoft office 2010	2	2,7	8,7	ALTO
43	PC -ARCHIVO CENTRO- windows xp 2002 microsoft office 2007	3	1,3	10,3	SUPERIOR
44	PC- Factcentro- windows 7 ultimate	3	2	8	ALTO
45	Pc -Citologias-windows 7 professional	2	2	6	MEDIO

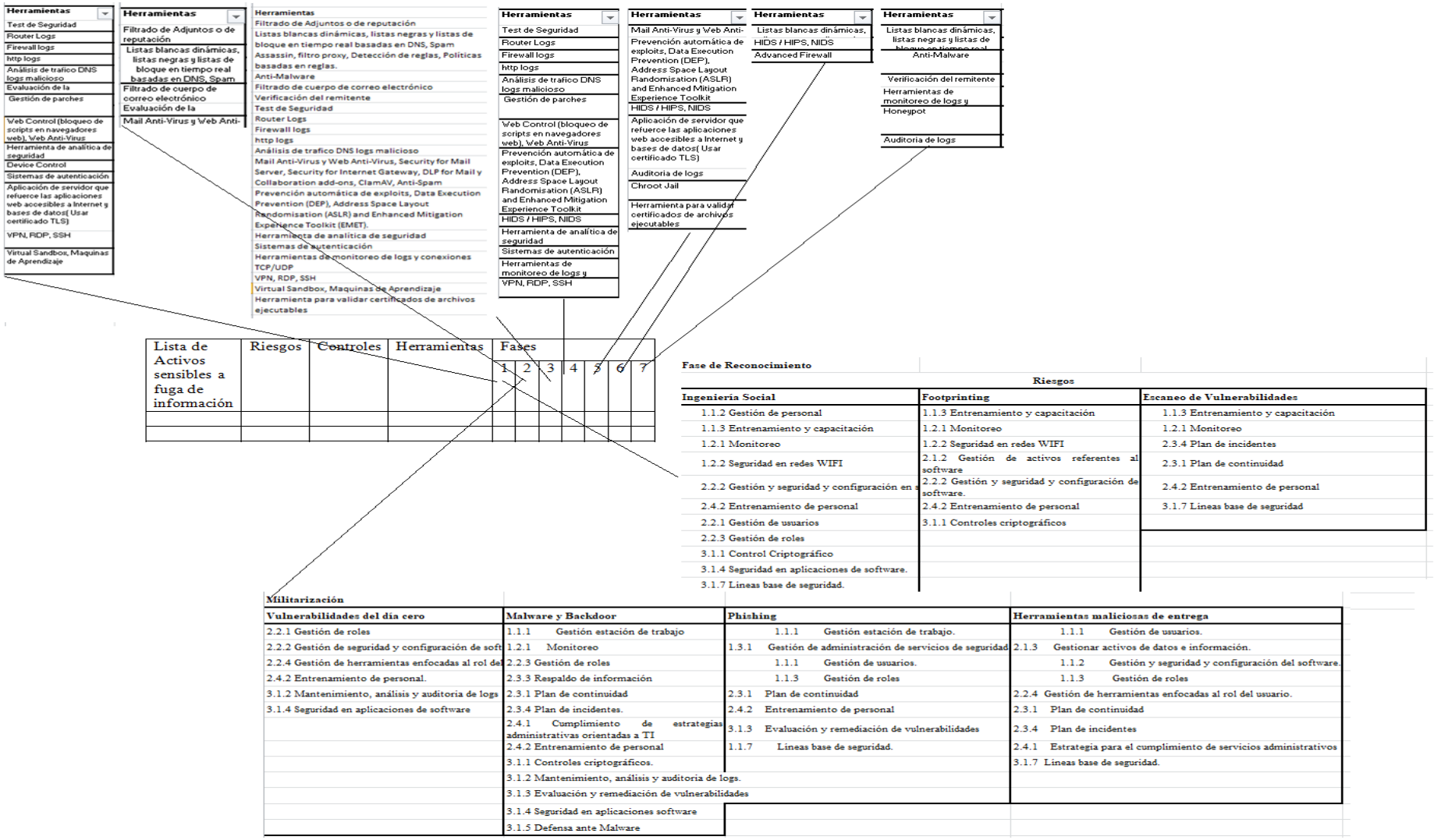
Tabla 53. Activos evaluados con la guía de identificación de activos sensibles a fuga

3.4.4. Inclusión de Buenas prácticas y Herramientas en cada fase del ciclo de vida del APT

Esta es la fase de final que permite aplicar los controles que surgieron de las buenas prácticas, como también recomienda herramientas para mitigar riesgos que se identificaron gracias al estudio que surgió en el ítem 3.2.1. Dichos elementos van enfocados a la fase del ciclo de vida del APT a las cuales aplica y donde sus activos pueden ser vulnerados. Ver siguiente iñustración 11 que permite aplicar controles pertinentes.

Aplicando controles y Herramientas en cada fase del ciclo de vida del APT a los activos sensibles a fuga de información con calificación Media, Alta y Superior.

Ilustración 11.Framework de Seguridad para mitigar APT en cada fase del ciclo de vida



3.5. Pruebas Del Framework

A continuación se muestran los resultados del framework propuesto, el cual se probó con activos de hospital de Santander de quilichao para permitir tener acceso a la información debido a que en Medellín ninguna entidad hospitalaria respondió a la solicitud, porque el sector Salud es muy delicado con brindar información; dado que esta muestra el estado real en cuanto a seguridad (Ver anexo D).

Para hacer las pruebas se debe seguir las recomendaciones de la guía que se propuso en el objetivo 1 de levantamiento de activos, objetivo 2 de Buenas prácticas, objetivo 3 de herramientas para mitigar la fuga de información ocasionada por APT. A continuación se muestra la información recolectada y clasificada.

Cabe anotar que el framework propone un conjunto de artefactos (Ver anexo A), buenas prácticas (Ver anexo B) y herramientas (Ver anexo C) para mitigar la fuga de información ocasiona por APT en los activos informáticos del sector hospitalario y en ningún caso se propuso como una herramienta técnica, si no como una guía estratégica para mitigar las APT, por tanto no se ejecutara un ataque para ver la funcionalidad de este, ya que en las herramientas que el framework propone son resultado de investigación de autores reconocidos que fueron tomadas como referencia y clasificadas según su nivel de protección. Es de resaltar que a todas las herramientas se le realizaron las pruebas pertinentes para combatir las APT que tienen vector de ataque correo electrónico. **Ver anexo C**. Es por ello que el framework se enfoca en que las entidades hospitalarias reduzcan los riesgos de que suceda un hecho de tal envergadura que pueda causar daño en su imagen y fuga de información en activos delicados y susceptibles a ser protegidos.

3.5.1. Pruebas clasificación de activos del hospital QUILISALUD

Para dichas pruebas se tomaron 90 activos entre tecnológicos e informáticos que estaban documentados en la entidad de salud, los cuales fueron valorados como se muestra en la tabla 72 siguiendo las recomendaciones de la guía de identificación de activos sensibles a fuga de información. Para más información ver anexo A, ítem 6.1.

QUILISALUD
NIT. 817.003.532-4
Servimos con calidad humana

Add a Record Export

82 Record(s)

Codigo Activo	Nombre	Descripcion Activo	Codigo Proceso	Tipo Activo	Ubicación	Responsable	Información	Formato	Valoración Confidencialidad	Valoración Integridad	Valoración Disponibilidad	Nivel Criticidad
7	Analizador de Quimica Clinica ...	con lector de barras de Muestr...	3	6	2	1	4	1	3	3	2	3
8	Analizador de Orina H500 DIRUI	Tecnología de celda de flujo p...	3	6	2	1	4	8	3	3	3	3
9	Analizador de Hematologia	3 Partes BC-3200 Marca: MINDRA...	3	6	2	1	4	8	3	3	3	3
10	Analizador Quimica A-15 S/N 83...	NAP MORALES DUQUE	3	6	2	1	3	8	3	3	3	3
11	Centrifuga de 24 Tubos C/Tacom...	Marca: LWSCIENTIFIC Serie:1506...	3	6	2	1	3	8	3	3	3	3
12	Omax 40x X Microscopio Binocul...	Marca LWSCIENTIFIC	3	6	2	1	3	8	3	3	3	3
13	Microcentrifuga ref. CT-1D	timer electronico digital,	3	6	2	1	3	8	3	2	2	3
14	Agitador de mazzini V Variable...	Marca Gemmy Model VRN-200	3	6	2	1	3	8	2	2	2	2
15	Cuenta globulos ref. CG 97, E...	teclado de alta sensibilidad, ...	3	6	2	1	3	8	2	2	2	2
16	Centrifuga 12 tubos CIENTIFIC	Modelo: LC045S S/N: 50619239	3	6	2	1	3	8	3	2	3	3
17	Centrifuga 12 tubos CIENTIFIC	Modelo: LC045S S/N: 50619239	3	6	2	1	3	8	3	2	2	3

18	Pipeta Volumen Variable 100-10...	Ninguna	3	6	2	1	1	1	1	0	0	1
19	Autoclave 12 Litros Digital M...	NAP CENTRO	3	6	4	1	1	1	1	0	0	1
20	Autoclave AUTOMAT 3000 S/300...	NAP MONDOMO	3	6	3	1	1	1	1	3	3	2
21	Autoclave AUTOMAT 3000 S/3000-...	EXTRAMURAL	3	6	4	1	1	1	1	2	3	1
22	Cavitron DENSTPLY S/N 130-3201...	NAP MONDOMO	3	6	4	1	1	1	1	1	1	1
23	Compresor SCHULZ MSV12 S/3209...	DOTACION DE EQUIPOS MEDICOS Y ...	3	6	4	1	1	1	1	0	2	1
24	DEA Desfibrilador Benehearth M...	NAP CENTRO	3	6	5	1	1	8	2	0	1	1
25	Detector Fetal FD-1 PANTALLA ...	NAP MONDOM	3	6	7	1	1	1	1	0	2	1
26	Detector Fetal (Dopler) Ref D...	NAP MORALES DUQUE	3	6	7	1	1	8	1	1	2	1
27	Ecografo EDAN DUS3 con transdu...	NAP MONDOMO	3	6	8	1	2	8	3	2	2	2
28	Electrocardiografo EDAN SE-3 S...	NAP MONDOMO	3	6	8	1	2	8	2	2	2	2
29	Equipo de rayos x ELITY 70 S/0...	NAP MONDOMO	3	6	4	1	3	8	3	2	2	3
30	Equipo de Escritorio SO. 8.1 ...	Intel pentium dual core E5700	1	3	4	3	3	8	4	3	3	3
31	Equipo de Escritorio SO. 8.1 ...	AMD Athlon 64 3000	1	3	4	3	3	8	4	2	3	3
32	Equipo Compaq 18 windows 8.1 P...	Intel Celeron j1800	1	3	4	3	4	8	4	3	3	3
33	Sony PAI_MONDOMO-PC windows 7...	Herramientas ofimáticas si	1	3	17	3	4	8	4	3	3	3
34	PC Sion Windows 7 ultimate	Tarjeta de RED si Herramienta ...	1	3	18	3	4	8	4	3	3	3
35	PC Sion MonCons3 Windows 8.1 ...	En red	1	3	19	3	3	8	3	3	3	3

Tabla 54. Lista de activos Hospital Quilisalud

3.5.2. Activos críticos

Se puede apreciar que la mayoría de activos clasificados como crítico son equipos cuyos sistemas operativos son Windows 7, XP y 2008 y manejan servidores con Windows server 2012, así mismo se identificó que tienen instalado la gran mayoría versiones de office 2007 que tienen vulnerabilidades conocidas al igual que los sistemas operativos.

Codigo Activo	Nombre Activo	Descripcion Activo	Nivel Criticidad
90	Software de Laboratorio	Prolag	3
89	Software de Historias Clìnicas	Historias Clínicas	3
88	Server Sip-Quili -linux Ubuntu...	linux Ubuntu 12	3
87	QUILISERVER-Windows Server Sta...	Windows Server Standard FE	3
86	PC-AUXILIAR DE CUENTAS-Windows...	Windows XP 2002 Microsoft Offi...	3
85	PC-HTA-Windows 7 Professional ...	Windows 7 Professional Microso...	2
84	PC-CALIDAD	Windows 7 Professional Microso...	3
83	PC-ENFNARINO-Windows 7professi...	Windows 7professional Microsof...	2
82	PC-ENFMORALES-Windows 7 profes...	Windows 7 professional Microso...	2
81	PC-QUILISALUD ESE-windows XP T...	windows XP Titan Ultimate Micr...	3
80	PC-SIAU-windows Xp Microsoft o...	windows Xp Microsoft office	2
79	PC-CON2MOR- windows 8.1 Micros...	windows 8.1 Microsoft Office 2...	3
78	Pc-HIPERTENCIONMORALES-Windows...	Windows 2007 -Microsoft Office...	2
77	PC -Consultorio-pc-Windows 7 P...	Windows 7 Professional -Micros...	3
76	PC-CONSULTORIO-Windows 8 Micro...	Windows 8 Microsoft office 201...	3
75	PC-Consult2-Windows 7 profesio...	Windows 7 profesional Microsof...	3
74	QuiliServer2-windows Server 20...	windows Server 2012 R2 Standar	3
73	PC- Copaso	windows 7 professional ,Micros...	3
72	PC-ODONTNAR-windows 8.1 pro Mi...	Windows 8.1 Pro Microsoft offi...	3
71	PC-COORDPYP-windows 7 ultimate...	windows 7 ultimate Microsoft o...	3
70	PC-Saludoral-windows 7 profess...	windows 7 professional Microso...	3
69	PC-Anexo3-windows 7 profession...	windows 7 professional	2
68	PC-VACUNACIÓN-windows 7 Profes...	windows 7 Profesional Microsof...	2
67	Pc-SIAU_NAR-windows 8.1Pro Mic...	windows 8.1Pro Microsoft Offic...	2
66	PC -CONSU_QNAR-windows 8.1 pro...	windows 8.1 pro Microsoft Offi...	3
65	PC-CON2NAR-windows 8.1pro Micr...	windows 8.1pro Microsoft Offic...	3
63	PC-LABORATORIO- windows Xp pro...	windows Xp profesional Office ...	3
62	Pc- Qulisalud-Cordinadora-wind...	windows Xp Microsoft office	3
61	PC-Consult4MOR -Windows 8.1 Pr...	Windows 8.1 Pro Microsoft offi...	3
60	PC- CONSULT3MOR -windows 8.1 p...	windows 8.1 pro Microsoft Offi...	3
59	PC- ENF2MOR- Windows 8.1 pro M...	Doctor-Windows 8.1 pro Microso...	3

Tabla 55. Activos críticos

3.5.3. Activos vs Amenazas

La mayoría de activos que pertenecen al laboratorio clínico, como lo son analizadores y máquinas de rayos x, están instalados a un equipo Windows cuyo sistema operativo es 2007 y tiene versiones de office con vulnerabilidades sin parchar. Sin embargo las amenazas sobre esos activos se clasificaron como errores de administrador, aunque puede haber otras amenazas presentes pero a consecuencia de estar conectados a un equipo que se puede infectar. Nota: *En esta sección solo se tiene un resumen de las pruebas realizadas, si desean*

conocer más al respecto remítase a la página de anexos D, pruebas de framework.

Activos VS Amenzas

Add a Record Export

Search

Save Changes

73 Record(s)

Codigo A A	Nombre Activo	EA	ERE	FI	SI	AP	ES	INE
7	Analizador de Quimica Clinica ...	☑	☐	☐	☐	☐	☐	☑
8	Analizador de Orina H500 DIRUI	☑	☐	☐	☐	☐	☐	☑
9	Analizador de Hematologia	☑	☐	☐	☐	☐	☐	☑
10	Analizador Quimica A-15 S/N 83...	☑	☐	☐	☐	☐	☐	☑
11	Centrifuga de 24 Tubos C/Tacom...	☑	☐	☐	☐	☐	☐	☐
12	Omax 40x X Microscopio Binocul...	☑	☐	☐	☐	☐	☐	☐
13	Microcentrifuga ref. CT-1D	☑	☐	☐	☐	☐	☐	☐
14	Agitador de mazzini V Variable...	☑	☐	☐	☐	☐	☐	☐
15	Cuenta globulos ref. CG 97, E...	☑	☐	☐	☐	☐	☐	☐
16	Centrifuga 12 tubos CIENTIFIC	☐	☐	☐	☐	☐	☐	☐
17	Centrifuga 12 tubos CIENTIFIC	☑	☐	☐	☐	☐	☐	☐
20	Autoclave AUTOMAT 3000 S/300...	☑	☐	☐	☐	☐	☐	☐
27	Ecografo EDAN DUS3 con transdu...	☑	☐	☐	☐	☐	☐	☐
28	Electrocardiografo EDAN SE-3 S...	☑	☐	☐	☐	☐	☐	☐
29	Equipo de rayos x ELITY 70 S/0...	☑	☐	☐	☐	☐	☐	☑
30	Equipo de Escritorio SO. 8.1 ...	☑	☑	☑	☑	☑	☑	☑
31	Equipo de Escritorio SO. 8.1 ...	☑	☑	☑	☑	☑	☑	☑
32	Equipo Compaq 18 windows 8.1 P...	☑	☑	☑	☑	☑	☑	☑
33	Sony PAI_MONDOMO-PC windows 7...	☑	☑	☑	☑	☑	☑	☑
34	PC Sion Windows 7 ultimate	☑	☑	☑	☑	☑	☑	☑
35	PC Sion MonCons3 Windows 8.1 ...	☑	☑	☑	☑	☑	☑	☑
36	PC FACTURACIÓNMOND Windows xp,...	☑	☑	☑	☑	☑	☑	☑
37	PC Compumax FACTURACION CENTRO...	☑	☑	☑	☑	☑	☑	☑
38	PC Lenovo- Windows 8.1 single ...	☑	☑	☑	☑	☑	☑	☑
39	Pc- SAMSUNG- Contabilidad- Win...	☑	☑	☑	☑	☑	☑	☑
40	Pc-Contratacion -windows 7 ult...	☑	☑	☑	☑	☑	☑	☑

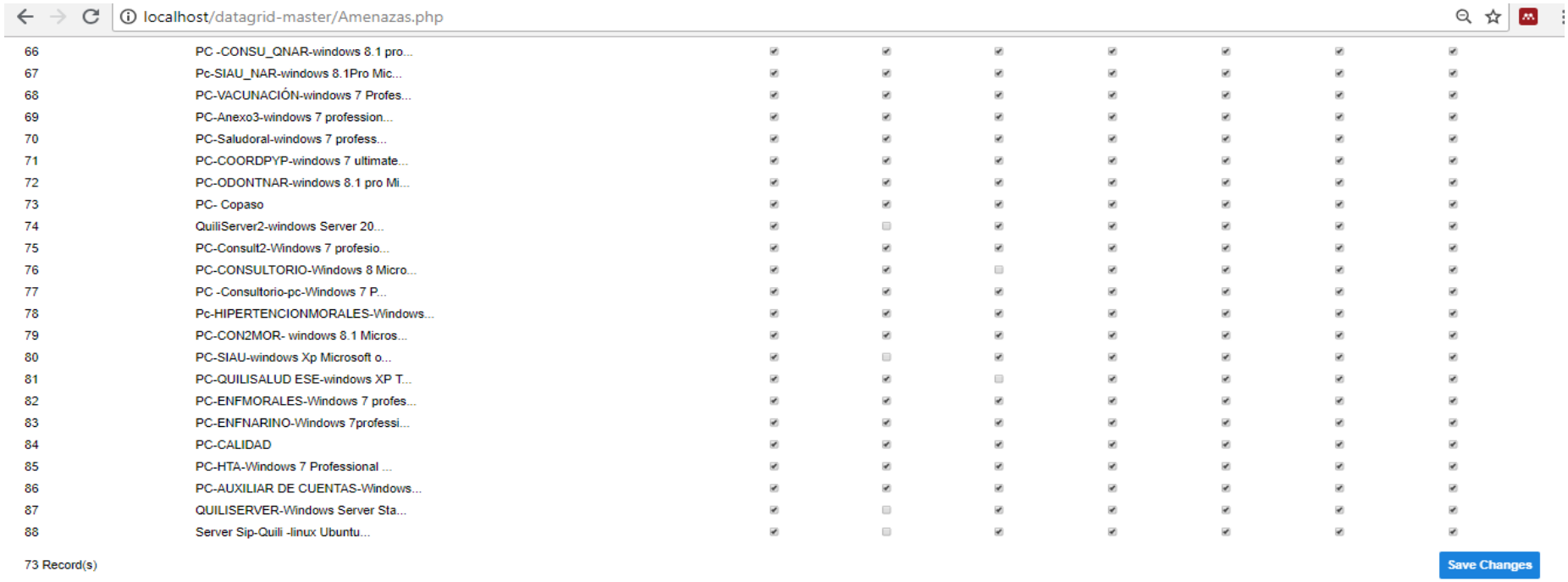


Tabla 56. Activos con amenazas posibles

3.5.4. Calculando nivel de fuga

Se puede apreciar en las tablas 75 que los equipos de escritorio con nivel de fuga medio, alto y superior deben ser protegidos debido a que sus sistemas operativos y software pueden tener vulnerabilidades conocidas. Por lo tanto es necesario hacer actualizaciones en dichos sistemas. A continuación se muestra la salida que arroja como insumo el framework, que le va servir como entrada para aplicar controles y herramientas a los riesgos asociados a las amenazas modeladas para dicho framework.

	Codigo_a	Nombre Activo	Sensibilidad_activo	Nivel_fuga	
2	7	Analizador de Quimica Clinica SELECTRA PROS Con modulo ISE	0,6	0,6	INFERIOR
3	8	Analizador de Orina H500 DIRUI	0,6	0,6	INFERIOR
4	9	Analizador de Hematologia	0,6	0,6	INFERIOR
5	10	Analizador Quimica A-15 S/N 831051483	0,6	0,6	INFERIOR
6	11	Centrifuga de 24 Tubos C/Tacometro Digital	0,6	0,6	INFERIOR
7	12	Omax 40x X Microscopio Binocular Compuesto De Laboratorio C	0,6	0,6	INFERIOR
8	13	Microcentrifuga ref. CT-1D	0,6	0,6	INFERIOR
9	14	Agitador de mazzini V Variable 803621	0,6	0,6	INFERIOR
10	15	Cuenta globulos ref. CG 97, Equipo Electronico digital	0,6	0,6	INFERIOR
11	16	Centrifuga 12 tubos CIENTIFIC	0,6	0,6	INFERIOR
12	17	Centrifuga 12 tubos CIENTIFIC	0,6	0,6	INFERIOR
13	20	Autoclave AUTOMAT 3000 S/3000-0692	0,6	0,6	INFERIOR
14	27	Ecografo EDAN DUS3 con transductor convexo s/317206-M13101620001	0,6	0,6	INFERIOR
15	28	Electrocardiografo EDAN SE-3 S/SE3B323113140611,	0,6	0,6	INFERIOR
16	29	Equipo de rayos x ELITY 70 S/0234, con negatoscopio	0,6	0,6	INFERIOR
17	30	Equipo de Escritorio SO. 8.1 pro	2	6	MEDIO
18	31	Equipo de Escritorio SO. 8.1 pro	2	6	MEDIO
19	32	Equipo Compaq 18 windows 8.1 Pro	2	6	MEDIO
20	33	Sony PAI_MONDOMO-PC windows 7 professional	1,3	5,3	MEDIO
21	34	PC Sion Windows 7 ultimate	2	6	MEDIO
22	35	PC Sion MonCons3 Windows 8.1 pro, Microsoft office 2013	2	6	MEDIO
23	36	PC FACTURACIÃ“NMOND Windows xp, Microsoft Office 2007	2	6	MEDIO
24	37	PC Compumax FACTURACION CENTRO windows 2007, Microsoft office 2007	2	6	MEDIO
25	38	PC Lenovo- Windows 8.1 single language Microsoft office 2010	2	4	BAJO

activos_Criticos_quilisalud | Nivel Fuga

Continuación salida de resultados con nivel de fuga.

24	37	PC Compumax FACTURACION CENTRO windows 2007, Microsoft office 2007	2	6	MEDIO
25	38	PC Lenovo- Windows 8.1 single language Microsoft office 2010	2	4	BAJO
26	39	Pc- SAMSUNG- Contabilidad- Windows 2007 Microsoft office 2003	2	6	MEDIO
27	40	Pc-Contratacion -windows 7 ultimate microsoft office 2010	2	6	MEDIO
28	41	Pc- Citologia- windows 8,1 pro microsoft 0ffice 2010	2,7	6,7	MEDIO
29	42	Pc -sistemas2 -windows 10 microsoft office 2010	2,7	8,7	ALTO
30	43	PC -ARCHIVO CENTRO- windows xp 2002 microsoft office 2007	1,3	10,3	SUPERIOR
31	44	PC- Factcentro- windows 7 ultimate	2	8	ALTO
32	45	Pc -Citologias-windows 7 professional	2	6	MEDIO
33	46	PC- Quili_pic- Coordinador Sistemas	1,3	7,3	ALTO
34	47	PC- Secretaria	1,3	10,3	SUPERIOR
35	48	PC -Presupuesto -windows Xp Microsoft	1,3	5,3	MEDIO
36	49	PC -MINISTERIO DE LA PROTEC- windows Xp Microsoft	1,3	5,3	MEDIO
37	50	Pc- Tesorero- windows Xp Microsoft Office 2017	1,3	5,3	MEDIO
38	51	Pc - Coordcenter-Jefe-windows 7 pro	1,3	10,3	SUPERIOR
39	52	Pc- CONS2_CENTRO - Windows 8.1 Pro Microsoft office 2010	2	6	MEDIO
40	53	Pc- PRECENT-Windows 7 profesional Microsoft office 2007	1,3	5,3	MEDIO
41	54	Pc- Vacunacion- windows 7 profesional Microsoft	2	5	MEDIO
42	55	Pc- Quilisalud4- windows Xp	2	8	ALTO
43	56	Pc- Usuario- windows 8.pro	2,7	6,7	MEDIO
44	57	Pc- Odontcentro2- Windows 8.1 pro	2,7	4,7	BAJO
45	58	Pc- MONENFERM -Windows 7 profesional Microsoft office 2010	1,3	5,3	MEDIO
46	59	PC- ENF2MOR- Windows 8.1 pro Microsoft Office 2010	2	6	MEDIO
47	60	PC- CONSULT3MOR -windows 8.1 pro Microsoft Office 2010	2	6	MEDIO
48	61	PC-Consult4MOR -Windows 8.1 Pro Microsoft office 2010	2	6	MEDIO

Tabla 57. Calculando nivel de fuga de información

Fuente de elaboración propia

3.5.5. Activos con nivel de fuga de información considerado como Medio, Alto y Superior.

De los 90 activos registrados se obtuvieron 59 con nivel de fuga considerado como riesgoso para la entidad hospitalaria. Así mismo se aprecia que los sistemas más críticos son los equipos que tiene sistema operativo XP y sirven al área de archivo y secretaria donde reposa información de usuarios del sistema, también se encontró que el equipo que posee el coordinador del área de sistemas del hospital tiene un nivel de fuga superior, al igual que el software de historias clínicas y de laboratorio, debido a que reposa toda la historia clínica de pacientes y exámenes médicos que son confidenciales, y que acceden los médicos desde los pc que tienen instalado sistemas operativos sin soporte.

A continuación se muestran los activos sensibles a fuga de información.

1	Codigo	Nombre Activo	Codigo_Impact	Sensibilidad_activo	Nivel_fuga	Calificació
17	30	Equipo de Escritorio SO. 8.1 pro	2	2	6	MEDIO
18	31	Equipo de Escritorio SO. 8.1 pro	2	2	6	MEDIO
19	32	Equipo Compaq 18 windows 8.1 Pro	2	2	6	MEDIO
20	33	Sony PAI_MONDOMO-PC windows 7 professional	2	1,3	5,3	MEDIO
21	34	PC Sion Windows 7 ultimate	2	2	6	MEDIO
22	35	PC Sion MonCons3 Windows 8.1 pro, Microsoft office 2013	2	2	6	MEDIO
23	36	PC FACTURACIÃ“NMOND Windows xp, Microsoft Office 2007	2	2	6	MEDIO
24	37	PC Compumax FACTURACION CENTRO windows 2007, Microsoft office 2007	2	2	6	MEDIO
26	39	Pc- SAMSUNG- Contabilidad- Windows 2007 Microsoft office 2003	2	2	6	MEDIO
27	40	Pc-Contratacion -windows 7 ultimate microsoft office 2010	2	2	6	MEDIO
28	41	Pc- Citologia- windows 8,1 pro microsoft 0ffice 2010	2	2,7	6,7	MEDIO
29	42	Pc -sistemas2 -windows 10 microsoft office 2010	2	2,7	8,7	ALTO
30	43	PC -ARCHIVO CENTRO- windows xp 2002 microsoft office 2007	3	1,3	10,3	SUPERIOR
31	44	PC- Factcentro- windows 7 ultimate	3	2	8	ALTO
32	45	Pc -Citologias-windows 7 professional	2	2	6	MEDIO
33	46	PC- Quili_pic- Coordinador Sistemas	3	1,3	7,3	ALTO
34	47	PC- Secretaria	3	1,3	10,3	SUPERIOR
35	48	PC -Presupuesto -windows Xp Microsoft	2	1,3	5,3	MEDIO
36	49	PC -MINISTERIO DE LA PROTEC- windows Xp Microsoft	2	1,3	5,3	MEDIO
37	50	Pc- Tesorero- windows Xp Microsoft Office 2017	2	1,3	5,3	MEDIO
38	51	Pc - Coordcenter-Jefe-windows 7 pro	3	1,3	10,3	SUPERIOR
39	52	Pc- CONS2_CENTRO - Windows 8.1 Pro Microsoft office 2010	2	2	6	MEDIO

40	53	Pc- PRECENT-Windows 7 profesional Microsoft office 2007	2	1,3	5,3	MEDIO
41	54	Pc- Vacunacion- windows 7 profesional Microsoft	1	2	5	MEDIO
42	55	Pc- Quilisalud4- windows Xp	2	2	8	ALTO
43	56	Pc- Usuario- windows 8.pro	2	2,7	6,7	MEDIO
45	58	Pc- MONENFERM -Windows 7 profesional Microsoft office 2010	2	1,3	5,3	MEDIO
46	59	PC- ENF2MOR- Windows 8.1 pro Microsoft Office 2010	2	2	6	MEDIO
47	60	PC- CONSULT3MOR -windows 8.1 pro Microsoft Office 2010	2	2	6	MEDIO
48	61	PC-Consult4MOR -Windows 8.1 Pro Microsoft office 2010	2	2	6	MEDIO
49	62	Pc- Qulisalud-Cordinadora-windows Xp Microsoft office	2	2	8	ALTO
50	63	PC-LABORATORIO- windows Xp profesional Office 2007	3	2	11	SUPERIOR
51	65	PC-CON2NAR-windows 8.1pro Microsoft Office 2010	2	2	6	MEDIO
52	66	PC -CONSU_QNAR-windows 8.1 pro Microsoft Office 2010	2	2	6	MEDIO
53	67	Pc-SIAU_NAR-windows 8.1Pro Microsoft Office 2010	2	2	6	MEDIO
55	69	PC-Anexo3-windows 7 professional	2	2	6	MEDIO
56	70	PC-Saludoral-windows 7 professional -Microsoft oficce	1	2	5	MEDIO
57	71	PC-COORDPYP-windows 7 ultimate Microsoft office 2010	2	2	8	ALTO
58	72	PC-ODONTNAR-windows 8.1 pro Microsoft office 2010	2	2	6	MEDIO
59	73	PC- Copaso	2	2	6	MEDIO
60	74	QuiliServer2-windows Server 2012 R2 Standar	3	3,4	12,4	SUPERIOR
61	75	PC-Consult2-Windows 7 profesional -Microsoft office 2007	2	2	8	ALTO
62	76	PC-CONSULTORIO-Windows 8 Microsoft office 2010	2	2,7	6,7	MEDIO
63	77	PC -Consultorio-pc-Windows 7 Professional -Microsoft Office 2010	2	2,7	6,7	MEDIO
64	78	Pc-HIPERTENCIONMORALES-Windows 2007 Microsoft Office 2007	2	2	6	MEDIO
65	79	PC-CON2MOR- windows 8.1 Microsoft Office 2010	2	2,7	6,7	MEDIO
66	80	PC-SIAU-windows Xp Microsoft office	2	2,7	8,7	ALTO
67	81	PC-QUILISALUD ESE-windows XP Titan Ultimate Microsoft Office 2007	2	2	8	ALTO
68	82	PC-ENFMORALES-Windows 7 professional Microsoft Office 2010	2	2,7	8,7	ALTO
69	83	PC-ENFNARINO-Windows 7professional Microsoft Office 2010	2	2,7	6,7	MEDIO
70	84	PC-CALIDAD	2	2,7	6,7	MEDIO
71	85	PC-HTA-Windows 7 Professional Microsoft Office 2007	2	2	6	MEDIO
72	86	PC-AUXILIAR DE CUENTAS-Windows XP 2002 Microsoft Office 2007	2	2,7	6,7	MEDIO
73	87	QUILISERVER-Windows Server Standard FE	3	3,4	12,4	SUPERIOR
74	88	Server Sip-Quili -linux Ubuntu 12	3	2	8	ALTO
75	90	Software de Laboratorio Clinico	3	3,4	12,4	SUPERIOR
76	89	Software de Historias Clinicas	3	3,4	12,4	SUPERIOR

Tabla 58.Activos con considerable nivel de fuga de información

Si desean mayor información al respecto se sugiere que se remita al anexo D, ítem 6.4.

Luego de tener los resultados de los activos sensibles se procede a extraer los activos que pueden estar expuestos a las amenazas que fueron modeladas en la guía de identificación de activos. A continuación se muestra la siguiente tabla que muestra dicha asociación.

Extracción de las amenazas de los activos comprometidos

Codigo_A_A	Nombre_activo	AMENAZAS						
7	Analizador de Quimica Clinica SELECTRA PROS Con	EA						INE
8	Analizador de Orina H500 DIRUI	EA						INE
9	Analizador de Hematologia	EA						INE
10	Analizador Quimica A-15 S/N 831051483	EA						INE
11	Centrifuga de 24 Tubos C/Tacometro Digital	EA						
12	Omax 40x X Microscopio Binocular Compuesto De Lat	EA						
13	Microcentrifuga ref. CT-1D	EA						
14	Agitador de mazzini V Variable 803621	EA						
15	Cuenta globulos ref. CG 97, Equipo Electronico digital	EA						
16	Centrifuga 12 tubos CIENTIFIC	EA						
17	Centrifuga 12 tubos CIENTIFIC	EA						
20	Autoclave AUTOMAT 3000 S/3000-0692	EA						
27	Ecografo EDAN DUS3 con transductor convexo s/317	EA						
28	Electrocardiografo EDAN SE-3 S/SE3B323113140611,	EA						
29	Equipo de rayos x ELITY 70 S/0234, con negatoscopio	EA						INE
30	Equipo de Escritorio SO. 8.1 pro	EA	ERE	FI	SI	AP	ES	INE
31	Equipo de Escritorio SO. 8.1 pro	EA	ERE	FI	SI	AP	ES	INE
32	Equipo Compaq 18 windows 8.1 Pro	EA	ERE	FI	SI	AP	ES	INE
33	Sony PAL_MONDOMO-PC windows 7 professional	EA	ERE	FI	SI	AP	ES	INE
34	PC Sion Windows 7 ultimate	EA	ERE	FI	SI	AP	ES	INE
35	PC Sion MonCons3 Windows 8.1 pro, Microsoft office 2	EA	ERE	FI	SI	AP	ES	INE
36	PC FACTURACIÃ“NMOND Windows xp, Microsoft Offic	EA	ERE	FI	SI	AP	ES	INE
37	PC Compumax FACTURACION CENTRO windows 200	EA	ERE	FI	SI	AP	ES	INE
38	PC Lenovo- Windows 8.1 single language Microsoft off	EA	ERE	FI	SI	AP	ES	INE
39	Pc- SAMSUNG- Contabilidad- Windows 2007 Micros	EA	ERE	FI	SI	AP	ES	INE
40	Pc-Contratacion -windows 7 ultimate microsoft office	EA	ERE	FI	SI	AP	ES	INE
41	Pc- Citologia- windows 8,1 pro microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
42	Pc -sistemas2 -windows 10 microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE
43	PC -ARCHIVO CENTRO- windows xp 2002 microsoft o	EA	ERE	FI	SI	AP	ES	INE
44	PC- Factcentro- windows 7 ultimate	EA	ERE	FI	SI	AP	ES	INE
45	Pc -Citologias-windows 7 professional	EA	ERE	FI	SI	AP	ES	INE
46	PC- Quili_pic- Coordinador Sistemas	EA	ERE	FI	SI	AP	ES	INE
47	PC- Secretaria	EA	ERE	FI	SI	AP	ES	INE
48	PC -Presupuesto -windows Xp Microsoft	EA	ERE	FI	SI	AP	ES	INE
49	PC -MINISTERIO DE LA PROTEC- windows Xp Micros	EA	ERE	FI	SI	AP	ES	INE
50	Pc- Tesorero- windows Xp Microsoft Office 2017	EA	ERE	FI	SI	AP	ES	INE
51	Pc - Coordcenter-Jefe-windows 7 pro	EA	ERE	FI	SI	AP	ES	INE
52	Pc- CONS2_CENTRO - Windows 8.1 Pro Microsoft offi	EA	ERE	FI	SI	AP	ES	INE
53	Pc- PRECENT-Windows 7 profesional Microsoft office	EA	ERE	FI	SI	AP	ES	INE
54	Pc- Vacunacion- windows 7 profesional Microsoft	EA	ERE	FI	SI	AP	ES	INE
55	Pc- Quilisalud4- windows Xp	EA	ERE	FI	SI	AP	ES	INE
56	Pc- Usuario- windows 8.pro	EA	ERE	FI		AP	ES	INE
57	Pc- Odontcentro2- Windows 8.1 pro	EA	ERE	FI	SI	AP	ES	INE
58	Pc- MONENFERM -Windows 7 profesional Microsoft o	EA	ERE	FI	SI	AP	ES	INE
59	PC- ENF2MOR- Windows 8.1 pro Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
60	PC- CONSULT3MOR -windows 8.1 pro Microsoft Offic	EA	ERE	FI	SI	AP	ES	INE
61	PC-Consult4MOR -Windows 8.1 Pro Microsoft office 2	EA	ERE	FI	SI	AP	ES	INE
62	Pc- Qulisalud-Cordinadora-windows Xp Microsoft offi	EA	ERE	FI	SI	AP	ES	INE
63	PC-LABORATORIO- windows Xp profesional Office 2	EA	ERE	FI	SI	AP	ES	INE
65	PC-CON2NAR-windows 8.1pro Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
66	PC -CONSU_QNAR-windows 8.1 pro Microsoft Office	EA	ERE	FI	SI	AP	ES	INE
67	Pc-SIAU_NAR-windows 8.1Pro Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
68	PC-VACUNACIÃ“N-windows 7 Profesional Microsoft O	EA	ERE	FI	SI	AP	ES	INE

Tabla 59.Activos con nivel fuga críticos y con posibles amenazas

3.5.6. Activos con los respectivos riesgos de acuerdo a la amenza que lo relaciona.

El resultado final se aprecia en la siguiente tabla y en el anexo D, donde se puede visualizar los activos con su respectivo nivel de fuga y los riesgos a los cuales está expuesto cada activo de la organización objeto de esta prueba. Para evitar que se presente una vulneración es necesario incluir las buenas prácticas y herramientas que se encuentran en la sección 3.4.4.

Activos sensibles a fuga de información identificados según sus riesgos y amenazas a las cuales se les debe incluir recomendaciones dadas en la sección de buenas prácticas y herramientas.

Codigo_activo	Nombre Activo	Codigo_Impacto	Sensibilidad_activo	Nivel_fuga	Calificación	EA	ERE	FI	SI	AP	ES	INE
30	Equipo de Escritorio SO. 8.1 pro	2	2	6	MEDIO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingenieria social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingenieria social-Phishing	Pérdida de integridad de datos
31	Equipo de Escritorio SO. 8.1 pro	2	2	6	MEDIO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingenieria social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingenieria social-Phishing	Pérdida de integridad de datos
32	Equipo Compaq 18 windows 8.1 Pro	2	2	6	MEDIO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingenieria social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingenieria social-Phishing	Pérdida de integridad de datos
33	Sony PAI_MONDOMO-PC windows 7 professional	2	1,3	5,3	MEDIO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingenieria social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingenieria social-Phishing	Pérdida de integridad de datos
34	PC Sion Windows 7 ultimate	2	2	6	MEDIO	Footprinting - Escaneo de	Vulnerabilidades del dia cero-	Robo de información	Herramientas maliciosas de	Escalar privilegios-Ejecución de malware-Instalación y	Ingenieria social-Phishing	Pérdida de integridad de

PC-HTA-Windows 7 Professional Microsoft Office 2007	2	2	6	MEDIO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC-AUXILIAR DE CUENTAS-Windows XP 2002 Microsoft Office 2007	2	2,7	6,7	MEDIO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
QUILISERVER-Windows Server Standard FE	3	3,4	12,4	SUPERIOR	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	0	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
Server Sip-Quili -linux Ubuntu 12	3	2	8	ALTO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	0	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
Software de Laboratorio Clinico	3	3,4	12,4	SUPERIO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	0	Robo de información	0	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
Software de Historias Clinicas	3	3,4	12,4	SUPERIO	Footprinting - Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	0	Robo de información	0	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

Tabla 60. Activos con sus respectivos riesgos

3.5.7. Análisis de resultados

En esta sección se presenta la funcionalidad del framework propuesto con cada una de sus fases, además explica cómo las secciones anteriores se enlazan al marco propuesto. También se presentan las pruebas realizadas a los activos de un centro hospitalario real y donde se confirma la validez y aplicabilidad del framework de seguridad que se propuso, que fue capaz de identificar una serie de riesgos en dichos activos, a los cuales se les debe aplicar las recomendaciones brindadas en el resultado 2 y 3 de esta tesis.

Los activos que se clasificaron como medios, altos y superior, son equipos que por lo general tienen versiones de Windows sin soporte técnico, además el hospital no tiene licencias y por eso son sistemas muy vulnerables según se puedo apreciar en las pruebas realizadas. Donde muchos de sus vulnerabilidades se enunciaron en la lista clasificada según los últimos sucesos de APT y se pueden relacionar fácilmente, pues muchos del software que han sido vulnerados, se aprecian en la descripción del activo.

Es de gran importancia entender los riesgos a los que pueden estar asociados los activos del sector hospitalario para evitar la fuga de información que según los resultados obtenidos en el sector salud, el riesgo de que suceda un evento con un APT enfocada en el sector salud es muy alto y puede comprometer la información clínica de los pacientes que es la que se mantuvo en un rango superior según los hallazgos.

Cabe mencionar que el 90% de activos identificados con el framework presentan riesgos como los son **Footprinting -Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recolección de credenciales de usuario.**

Es necesario aplicar los controles y herramientas para dichos riesgos como se propone en el framework para mitigar las amenazas persistentes avanzadas en la organización.

Los activos que presentaron riesgos superior son: el software de historias clínicas y de laboratorio, así mismo como los servidores que tienen sistema operativo Windows, en esta prueba llamado QUILISERVER-Windows Server Standard FE y equipos que tienen sistema operativo Windows xp.

4. Conclusiones y Recomendaciones

En esta tesis se propuso un framework de seguridad informática que permitió:

Proponer una estrategia que funciona bajo el concepto de DLP para identificar y clasificar los activos de información sensibles del sector hospitalario, que sean susceptibles a fuga de información ocasionada por APT, proveniente de correo electrónico. El resultado es la guía para la identificación de activos sensibles a fuga de información en el sector salud, lo que facilito enriquecer el análisis de riesgos de seguridad de la información y plantear controles de mitigación enmarcados en un plan de tratamiento, también permitió identificar cuáles son las vulnerabilidades más comunes. Por otra parte se determinó el nivel de sensibilidad de los activos, haciendo prioridad en las vulnerabilidades al cual están expuestos los activos que pueden ser objeto de una amenaza persistente avanzada.

También se logró una revisión de diferentes framework de seguridad de la información a partir de los cuales se elaboraron un conjunto de buenas prácticas y herramientas que van a permitir al sector salud mitigar la fuga de información ocasionada por APT proveniente de correo electrónico.

Se definió un conjunto de políticas y buenas prácticas que permiten mitigar la fuga de información en los activos sensibles del sector hospitalario, en cada una de las fases del ciclo de vida del APT y se caracterizó un kit de herramientas de acuerdo a la fase del ciclo de vida del APT, que le va a permitir a la entidad hospitalaria, dependiendo de la fase en la que se encuentre el ciclo del APT, hacer efectivas las buenas prácticas propuestas para el framework en el sector hospitalario.

Además se establecieron un conjunto de artefactos, herramientas y aspectos metodológicos para el framework, que fueron tenidos en cuenta para hacer las pruebas de este marco en la entidad hospitalaria tomada como referencia.

Por último se identificó y reconoció que en la entidad hospitalaria tomada como referencia sus activos informáticos presentan serios riesgos y un alto porcentaje de sensibilidad a fuga de información, por tanto es necesario seguir una serie de controles que se proponen al sector salud en Colombia, debido a que en la gran mayoría de entidades manejan plataformas similares y no tienen personal capacitado para enfrentar este tipo de ataques APT.

4.1. Trabajo Futuro

Esta tesis de grado es la base para continuar otras tesis de maestría y de pregrado que quieran continuar con la investigación futura, entre lo que se puede resaltar como trabajo futuro sería:

Hacer caracterización de herramientas que vayan surgiendo en el tiempo y de uso libre dedicadas al sector hospitalario que sean efectivas y que le permita a hospitales que no poseen los recursos adecuarse a su presupuesto y también es posible que de desarrolle una herramienta de software que permita controlar en tiempo real el estado de los activos, al tiempo que permita asignar controles automáticamente para ver estado de cumplimiento dentro de la entidad y así medir el nivel de madurez de la organización.

Teniendo en cuenta que las amenazas persistentes son cambiantes y las tecnologías en el sector hospitalario son arcaicas y no existen áreas de seguridad informática, es necesario que se actualicen y apliquen mecanismos de seguridad cómo reglas de firewall, IDS, IPS o sistemas que identifiquen y mitiguen dichos ataques. Además se sugiere, para la correcta aplicación de procedimientos del framework, contar con el personal capacitado y disponible que pueda verificar el cumplimiento de las buenas prácticas y herramientas para los riesgos encontrados.

.

5. Bibliografía

Abad-Aramburu, C. (2015). Aplicación de metodología de Análisis de Malware al caso de estudio de la Amenaza Avanzada Persistente (APT) "Octubre Rojo." Retrieved from http://reunir.unir.net/handle/123456789/2841

Ammar, M., Rizk, M., Abdel-Hamid, A., & Aboul-Seoud, A. K. (2016). A Framework for Security Enhancement in SDN-Based Datacenters. In *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1–4). IEEE. https://doi.org/10.1109/NTMS.2016.7792427

Antivirus Mejor. (2016). Escalado de privilegios. Retrieved from http://www.mejor-antivirus.es/terminologia-informatica/escalado-de-privilegios.html

Antiy Labs. (2012). Analysis Report on Flame Worm Samples Antiy Labs. Retrieved from http://www.antiy.net/media/reports/flame-analysis.pdf

Assante, M., & Lee, R. (2015). The Industrial Control System Cyber Kill Chain. Retrieved from https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Baca, G. (2016). Introducción a la Seguridad Informática, 1–60. Retrieved from https://latam.casadellibro.com/libro-introduccion-a-la-seguridad-informatica/9786077443445/5374663

Bermejo, P. (2016). Aplicación de Metodología de Malware para el Análisis de la amenaza avanzada persistente (APT) " Poison Ivy " Trabajo de Fin de Máster. Retrieved from http://reunir.unir.net/bitstream/handle/123456789/4738/GAVIRIA %2C PABLO ANDRES.pdf?sequence=1&isAllowed=y

Bhatt, P., & Yano, E. (2013). Analyzing Targeted Attacks using Hadoop applied to Forensic Investigation. https://doi.org/10.5769/C2013004

Bhatt, P., Yano, E., & Gustavsson, P. (2014). Towards a framework to detect multi-stage advanced persistent threats attacks. In *Proceedings - IEEE 8th International*

Symposium on Service Oriented System Engineering, SOSE 2014. https://doi.org/10.1109/SOSE.2014.53

Bodeau, D., & Graubart, R. (2013). Intended effects of cyber resiliency techniques on adversary activities. In *2013 IEEE International Conference on Technologies for Homeland Security, HST 2013*. https://doi.org/10.1109/THS.2013.6698967

Bravo, S., & Mauricio, D. (2018). DDoS Attack Detection Mechanism in the Application Layer Using User Features, 97–100. Retrieved from https://ieeexplore.ieee.org/document/8356848/

CAPEC. (2017). CAPEC - CAPEC Lista Versión 2.9. Retrieved April 29, 2017, from https://capec.mitre.org/data/index.html

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Retrieved from http://www.sei.cmu.edu/publications/pubweb.html

Carlos, G. (2010). Hablemos de Spoofing. Retrieved from https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

Centro Criptológico Nacional. (2018). CCN-STIC-821 Normas de Seguridad en el ENS. Apéndice I. Retrieved from https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/530-ccn-stic-821-normas-de-seguridad-en-el-ens-anexo-i/file.html

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-662-44885-4_5

Chen, X., Zhang, J., Wu, D., & Han, R. (2005). HIPPA's compliant Auditing System for Medical Imaging System. Retrieved from HIPPA's compliant Auditing System for Medical Imaging System

Colciencias. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informatica y de informacion bajo la norma ISO 27001. Retrieved from http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Colciencias. (2016). Manual inventario de activos, clasificaciòn y publicaciòn de la informaciòn. Retrieved from http://www.colciencias.gov.co/sites/default/files/upload/paginas/g104m02-manual-de-activos-de_-informacion.pdf

Cole, E. (2013). Proactive Security and Reputational Ranking. https://doi.org/10.1016/B978-1-59-749949-1.00010-3

Congreso Nacional de la República de Colombia. (2014). Ley 1712 de 2014, 1–14. Retrieved from http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY 1712 DEL 06 DE MARZO DE 2014.pdf

Costante, E., Fauri, D., Etalle, S., Den, H., & Zannone, N. (2016). A Hybrid Framework for Data Loss Prevention and Detection. https://doi.org/10.1109/SPW.2016.24

Costante, E., Fauri, D., Etalle, S., Hartog, J. Den, & Zannone, N. (2015). A Hybrid Framework for Data Loss Prevention & Detection. https://doi.org/10.1109/SPW.2016.24

Crowe, W. (2015). Cybersecurity Kill Chain. Retrieved from http://www.isaca.org/chapters2/jacksonville/events/Documents/CyberSecurity Kill Chain 8.19.15.pdf

Departamento Nacional de Planeación. (2016). Conpes 3854 - Política Nacional De Seguridad Digital. Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Econ﷿micos/3854.pdf

Direction centrale de la sécurité de systèmes d’information. (2003). El metodo Ebios. Retrieved from

https://www.ssi.gouv.fr/archive/es/confianza/documents/methods/ebiosv2-methode-plaquette-2003-09-01_es.pdf

Drinkwater, D. (2014). German iron plant hit by APT attack. Retrieved from https://www.scmagazineuk.com/german-iron-plant-hit-by-apt-attack/printarticle/540939/

FireEye. (2016a). Spear-Phishing Attacks Why They Are Successful And How To Stop Them. Retrieved from http://maxis360.com/wp-content/uploads/fireeye-how-stop-spearphishing.pdf

FireEye. (2016b). Threat Horizon & Industry Outlook. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/sb-healthcare-and-health-insurance.pdf

Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016). Social engineering attack strategies and defence approaches. *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 145–149. https://doi.org/10.1109/FiCloud.2016.28

Giura, P., & Wang, W. (2013). A context-based detection framework for advanced persistent threats. In *Proceedings of the 2012 ASE International Conference on Cyber Security, CyberSecurity 2012*. https://doi.org/10.1109/CyberSecurity.2012.16

Gupta, B., & Jyoti, K. (2014). Big Data Analytics with Hadoop to analyze Targeted Attacks on Enterprise Data. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=E3650E1775807AB9AE712C3CF4D8176C?doi=10.1.1.658.9394&rep=rep1&type=pdf

Gupta, S., Singhal, A., & Kapoor, A. (2017). A literature survey on social engineering attacks: Phishing attack. *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 537–540. https://doi.org/10.1109/CCAA.2016.7813778

HHS. (2017). Summary of the HIPAA Security Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Hutchins, E., Cloppert, M., & Amin, R. (n.d.). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

INCIBE. (2016). Cyber Kill Chain en Sistemas de Control Industrial. Retrieved March 27, 2017, from https://www.certsi.es/blog/cyber-kill-chain-sistemas-control-industrial

InfoSec Resources. (2015). What's Worse: APTs or Spear Phishing? Retrieved from https://resources.infosecinstitute.com/whats-worse-apts-or-spear-phishing/#gref

Instituto Ponemon. (2016). The state of cybersecurity in healthcare organizations in 2016.

Inteco. (2012). Esteganografía, el arte de ocultar información. *Instituto Nacional de Tecnologías de La Comunicación*, 1–15. Retrieved from http://www.egov.ufsc.br/portal/sites/default/files/esteganografia1.pdf

Ioannou, G., Louvieris, P., Clewley, N., & Powell, G. (2013). A Markov Multi-Phase Transferable Belief Model: An Application for predicting Data Exfiltration APTs. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6641081&isnumber=6641065

Ira, W., & Araceli, T. (2017). Countermeasures .Advanced Persistent Security. Retrieved from https://www.sciencedirect.com/science/article/pii/B9780128093160000105?via%3Dihub

Isaca. (2016). Vulnerando la política de seguridad de la información por diversión y dinero. Retrieved from https://www.isaca.org/Journal/archives/2017/Volume-

1/Pages/smashing-the-information-security-policy-for-fun-and-profit-spanish.aspx

ISACA. (2016). COBIT 5 Spanish. Retrieved from http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

ISO. (2016). ISO 27799:2016 - Health informatics -- Information security management in health using ISO/IEC 27002. Retrieved April 30, 2017, from https://www.iso.org/standard/62777.html

Jia, W. (2017). Study on Network Information Security Based on Big Data. In *2017 9th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)* (pp. 408–409). IEEE. https://doi.org/10.1109/ICMTMA.2017.0104

Jin, J., Ahn, G.-J., Hu, H., Covington, M., & Zhang, X. (2009). Patient-centric Authorization Framework for Sharing Electronic Health Records. Retrieved from https://people.cs.clemson.edu/~hongxih/papers/SACMAT09.pdf

Josep, A. (2015). ¿Sabes qué es un backdoor y en qué se diferencia de un troyano? Retrieved from https://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/

Karim, N. (2018). Riesgos en la seguridad informática en salud. Retrieved from http://www.elhospital.com/temas/Riesgos-en-la-seguridad-informatica-en-salud+111853?pagina=2

Kósa, A., Stuchlíková, L., & Benko, P. (2015). *Blended learning in preactise*. *Distance learning, simulation and communication 2015*. Retrieved from http://dlsc.unob.cz/data/Proceedings of the DLSC 2015 conference.pdf

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced Social Engineering Attacks. Retrieved from https://www.sba-research.org/wp-content/uploads/publications/jisa_revised.pdf

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering

attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Lab, K. (2015). Malicious Tools. Retrieved from https://www.kaspersky.es/resource-center/threats/malicious-tools

Lab, K. (2017). ¿Qué es el spear phishing? Retrieved from https://latam.kaspersky.com/blog/que-es-el-spear-phishing/12177/

Lee, K., Kim, J., Kwon, K. H., Han, Y., & Kim, S. (2008). DDoS attack detection method using cluster analysis. *Expert Systems with Applications*, *34*(3), 1659–1665. https://doi.org/10.1016/j.eswa.2007.01.040

Lee, R., Assante, M., & Conway, T. (2014). German Steel Mill Cyber Attack. Retrieved from https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Legalitas. (2016). Suplantación de identidad. Retrieved from https://www.legalitas.com/actualidad/suplantacion-de-identidad

Li, M., Huang, W., Wang, Y., Fan, W., & Li, J. (2016). The study of APT attack stage model. In *2016 IEEE/ACIS 15th International Conference on Computer and Information Science, ICIS 2016 - Proceedings*. https://doi.org/10.1109/ICIS.2016.7550947

Lockheed, M. (2014). The Modern Day Attacker. Retrieved from https://www.youtube.com/watch?v=Lyn50b_n0CY&list=UUJWcF0ex7_doPdIQGbVpDsQ

Lopez, N., & Ruiz, S. (2005). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved from http://www.iso27000.es/

Luca, G., Brattstrom, M., & Morreale, P. (2016). Designing a Secure e-Health Network System. Retrieved from https://ieeexplore.ieee.org/document/7490528/

Luh, R., Marschalek, S., Kaiser, M., Janicke, H., Schrittwieser, S., & Luh, B. R. (2017). Semantics-aware detection of targeted attacks: a survey. *Journal of Computer Virology and Hacking Techniques*, *13*, 47–85. https://doi.org/10.1007/s11416-016-0273-3

Marchetti, M., Guido, A., Pierazzi, F., & Colajanni, M. (2016). Countering Advanced Persistent Threats through security intelligence and big data analytics. In *International Conference on Cyber Conflict, CYCON*. https://doi.org/10.1109/CYCON.2016.7529438

Margaret, R. (2015). Prueba de penetración (pen test).

Matalobos, J. (2009). Analisis de Riegos Tessi. Retrieved from http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Mayer, P., & Leis, M. (2006). El correo electrónico en la relación médico-paciente. Retrieved from https://core.ac.uk/download/pdf/81215702.pdf

Medina, J. (2014). Evaluación de Vulnerabilidades TIC eBook: Javier Medina: Amazon.es: Tienda Kindle. Retrieved April 6, 2017, from https://www.amazon.es/Evaluación-Vulnerabilidades-TIC-Javier-Medina-ebook/dp/B00QGPIQHW

Meneses, B. (2007). De La Información, 65–118. Retrieved from http://www.tdx.cat/bitstream/handle/10803/8929/2LasnuevastecnologiasdelaInformacion.pdf;jsessionid=F45857BD94B5FF62A2C3AFED018A8167.tdx1?sequence=8

Messaoud, B., Guennoun, K., Wahbi, M., & Sadik, M. (2016). Advanced Persistent Threat: new analysis driven by life cycle phases and their challenges. Retrieved from https://ieeexplore.ieee.org/document/7843932/

Mifsud, E. (2012). Introducción a la seguridad informática - Vulnerabilidades de un sistema informático. Retrieved May 17, 2018, from http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-

introduccion-a-la-seguridad-informatica?start=3

Ministerio de Hacienda y Administraciones Públicas. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Retrieved from https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Ministerio de Hacienda y Administraciones Públicas, Centro Criptológico Nacional, M. de la P. de E. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método.

Ministerio de las TIC. (2016). Elaboración de la política general de seguridad y privacidad de la información.

Ministerio de Salud. (2016). REGISTRO DE APLICATIVOS DE INFORMACIÓN MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Retrieved April 9, 2017, from https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/OT/registro-aplicativos-informacion.pdf

MINTIC. (2010). Guía para la preparación de las TIC para la continuidad del negocio. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

MINTIC. (2016a). Guía de Auditoria. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

MINTIC. (2016b). Guía de gestión de riesgos. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MINTIC. (2016c). Guía de indicadores de gestión para la seguridad de la información. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

MINTIC. (2016d). Guía para la Gestión y Clasificación de Activos de Información. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MINTIC. (2016e). Guía para la Implementación de Seguridad de la Información en una MIPYME. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

MINTIC. (2016f). Procedimientos De Seguridad De La Información. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Moon, D., Im, H., Lee, J., & Park, J. (2014). MLDS: Multi-layer defense system for preventing advanced persistent threats. *Symmetry*. https://doi.org/10.3390/sym6040997

Mustafa, T. (2013). Malicious Data Leak Prevention and Purposeful Evasion Attacks: An approach to Advanced Persistent Threat (APT) management. *2013 Saudi International Electronics, Communications and Photonics Conference, SIECPC 2013*, 1–5. https://doi.org/10.1109/SIECPC.2013.6551028

Myers, L. (2015). ¿Qué es un 0-day? Explicando términos de seguridad. Retrieved from https://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/

Nazario, J. (2008). DDoS attack evolution. *Network Security*, *2008*(7), 7–10. https://doi.org/10.1016/S1353-4858(08)70086-2

Oprea, A., Li, Z., Yen, T., Chin, S., & Alrwais, S. (2015). Detection of Early-Stage Enterprise Infection by Mining Large-Scale Log Data. In *Proceedings of the International Conference on Dependable Systems and Networks*. https://doi.org/10.1109/DSN.2015.14

Pablo, G. (2018). *Ethical Hacking*. (OxWord, Ed.). Retrieved from https://0xword.com/es/libros/65-ethical-hacking-teoria-y-practica-para-la-realizacion-

de-un-pentesting.html

Prandini, M., & Ramilli, M. (2010). Towards a practical and effective security testing methodology. In *Proceedings - IEEE Symposium on Computers and Communications*. https://doi.org/10.1109/ISCC.2010.5546813

Raj, S. (2016). La "Segunda Economía" El Pronóstico para la Ciberseguridad del Sistema de la Salud. Retrieved from https://securingtomorrow.mcafee.com/languages/espanol/la-segunda-economia-el-pronostico-para-la-ciberseguridad-del-sistema-de-la-salud/

Ramírez, A., & Ortiz, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, *16*(2), 56–66. Retrieved from http://revistas.udistrital.edu.co/ojs/index.php/reving/article/view/3833

Rocío, N., Ríos, T., Janeth, D., Reyes, R., Leuvany, E., Morales, Á., … Miranda, M. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista Publicando*, (102), 462–473. Retrieved from http://www.rmlconsultores.com/revista/index.php/crv/article/viewFile/367/pdf_332

Rodriguez, J. (2015). Retos de seguridad en el sector salud. Retrieved from https://www.b-secure.co/blog/retos-de-seguridad-en-el-sector-salud

Sánchez, H., Fernández, J., Toval, A., Hernández, I., Sánchez, A., & Carrillo, J. (2014). *Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria*. *Atención Primaria* (Vol. 46). https://doi.org/10.1016/j.aprim.2013.10.008

Sethia, D., Gupta, D., & Saran, H. (2016). Security Framework for Portable NFC Mobile Based Health Record System. Retrieved from https://ieeexplore.ieee.org/document/7763175/

Shenwen, L., Yingbo, L., & Xiongjie, D. (2015). Study And Research of APT Detection

Technology Based on Big Data Processing Architecture. Retrieved from https://ieeexplore.ieee.org/document/7284547/

SIGEPRE. (2017). Guía Para La Calificación De La Información De Acuerdo Con Sus Niveles De Seguridad. Retrieved from http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf

Sotelo, B., Utrilla, J., & Ortega, J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. Retrieved from http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf

Symantec. (2018). New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia | Symantec Blogs. Retrieved May 19, 2018, from https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Tarazona, C. (2015). Amenazas Informáticas y seguridad de la informacion, 137–146. Retrieved from https://revistas.uexternado.edu.co/index.php/derpen/article/view/965

Thiranant, N., Sain, M., & Lee, H. (2013). A Design of Security Framework for Data Privacy in e-Health System using Web Service. Retrieved from http://onlinepresent.org/proceedings/vol38_2013/7.pdf

Trend Micro. (2012). Spear-phishing email : most favored APT attack bait, Trend Mciro incorporated research paper. *Ressearch Paper*, 1–8. Retrieved from http://www.trendmicro.co.uk/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Virvilis, N., & Gritzalis, D. (2013). The big four - What we did wrong in advanced persistent threat detection? In *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*. https://doi.org/10.1109/ARES.2013.32

Wang, X., Agham, S., Munishwar, V., Nipunage, V., Singh, S., & Gopalan, K. (2013). Transparent network protocol testing and evaluation. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*. https://doi.org/10.1109/ICCCN.2013.6614205

William F. Crowe, CISA, CISM , CRISC, C. (2015). CyberSecurity Kill Chain 8.19.15. Retrieved from http://www.isaca.org/chapters2/jacksonville/events/Documents/CyberSecurity Kill Chain 8.19.15.pdf

Wood, C., Hayden, S., Martinson, S., Kirkland, K., Alfonso, V., & Ardila, F. (2016). Conceptos básicos en buenas practicas en gestión de TI y seguridad de la información. Retrieved from http://www.it-docs.net/ddata/127.pdf

Xiangyu, L., Qiuyang, L., & Chandel, S. (2017). Social Engineering and Insider Threats. *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, *1*, 25–34. https://doi.org/10.1109/CyberC.2017.91

Yadav, T., & Rao, A. (2016). Technical Aspects of Cyber Kill Chain. https://doi.org/10.1007/978-3-319-22915-7

6. Anexos

6.1. Anexo A. Artefacto para hacer levantamiento de activos en el sector hospitalario

Artefacto para realizar levantamiento de Activos del sector Hospitalario que se propone en la guía.

Información Flexible								Información obligatoria					
Número Consecutivo	Nombre Activo	Descripción/Observaciones	Proceso	Tipo de Activo	Ubicación	Responsable	Tipo de información	Formato que Maneja	Valoración				Criticidad
								Seleccione Uno	Confidencialidad		Integridad	Disponibilidad	
1													
2													

Tabla 61. Artefacto de levantamiento de activos sensibles a fuga de información.

Fuente de elaboración propia

Valoración de activos y Amenazas propuestos para la guía.

Se propone el siguiente artefacto para realizar valoración de activo contra amenazas, que fueron homologadas y tomadas de acuerdo a margerit

Nombre del Activo	[EA]	[SI]	[AP]	[INE]	[ES]	[ES]

Leyendas			
[EA]	Errores de Administrador	[SI]	Suplantacion de identidad
[ERE]	Errores de Reencademamiento	[AP]	Usuarios Privelegiados
[FI]	Fuga de Informacion	[INE]	Interceptacion de información
		[ES]	Ingenieria Social

Fuente de elaboración Propia. Tabla 62.Valoración de activos Vs Amenazas cuyo vector de ataque es el correo electrónico

6.2. Anexo B. Buenas Prácticas y políticas.

Las salvaguardas Administrativas: Son prácticas diseñadas para controlar las medidas de seguridad y la conducta del personal que accede, se procesa y distribuye electrónicamente información médica protegida. Las salvaguardias Físicas: Son procesos que protegen equipo físico y edificios relacionados, de peligros naturales y medio ambientales, así como de intrusiones físicas. Salvaguardias Técnicas: Son mecanismos técnicos y procesos diseñados para proteger, controlar y monitorear el acceso a la información (HHS, 2017).

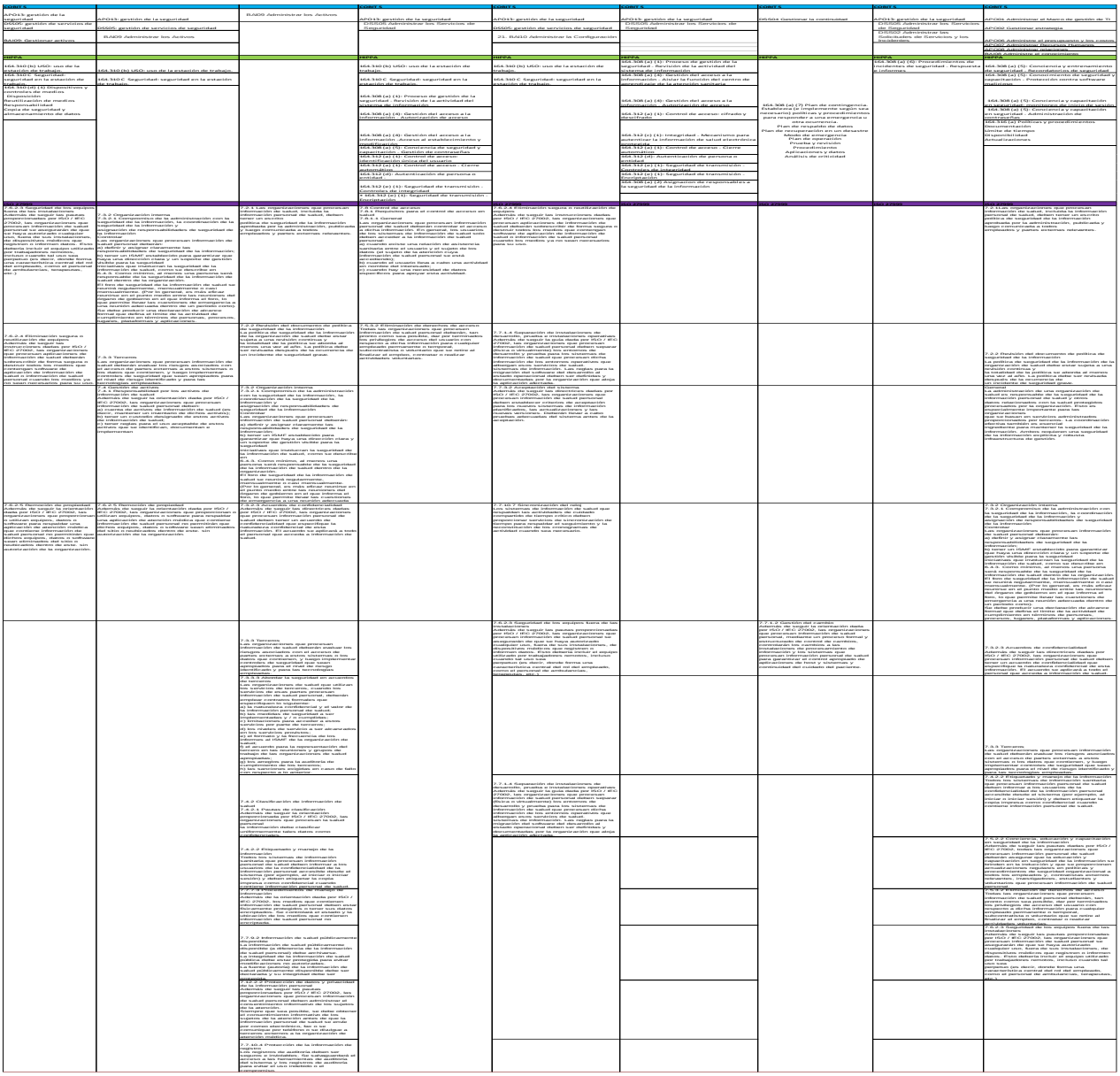
SALVAGUARDAS FISICAS		SALVAGUARDAS TECNICAS						
Limitacion y controles de puertos de red	Controles de acceso para wifi	Controles Criptograficos	Mantenimiento,monitoreo, analisis y auditoria de logs	Evaluacion, remediacion y gestión de vulnerabilidades	Seguridad en aplicaciones de Software	Lineas base de seguridad	Defensa ante Malware	Test de penetracion
ISO 27000								
9.1.2 Control de acceso a las redes y servicios asociados.	10.1.1 Política de uso de los controles criptográficos.	10.1.1 Política de uso de los controles criptográficos.	12.4.1 Registro y gestión de eventos de actividad.	12.6.1 Gestión de las vulnerabilidades técnicas.	9.4.5 Control de acceso al código fuente de los programas.	14.2.4 Restricciones a los cambios en los paquetes de software.	8.3.1 Gestión de soportes extraíbles.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
13.1.1 Controles de red.	12.4.1 Registro y gestión de eventos de actividad.	10.1.2 Gestión de claves	12.4.4 Sincronización de relojes.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	12.1.4 Separación de entornos de desarrollo, prueba y producción.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	12.2.1 Controles contra el código malicioso.	18.2.1 Revisión independiente de la seguridad de la información.
13.1.2 Mecanismos de seguridad asociados a servicios en red.	12.7.1 Controles de auditoría de los sistemas de información.		12.7.1 Controles de auditoría de los sistemas de información.		14.2.1 Política de desarrollo seguro de software.	18.2.3 Comprobación del cumplimiento.	13.2.3 Mensajería electrónica.	18.2.3 Comprobación del cumplimiento.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	13.1.3 Segregación de redes.				14.2.6 Seguridad en entornos de desarrollo.	10.1.1 Política de uso de los controles criptográficos.		
13.1.3 Segregación de redes.	14.1.3 Protección de las transacciones por redes telemáticas.				14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	12.3.1 Copias de seguridad de la información.		
						9.1.2 Control de acceso a las redes y servicios asociados.		
						12.4.1 Registro y gestión de eventos de actividad.		
						13.1.3 Segregación de redes.		
						12.7.1 Controles de auditoría de los sistemas de información.		
						13.2.3 Mensajería electrónica.		
						13.1.1 Controles de red.		
						8.3.1 Gestión de soportes extraíbles.		
						10.1.2 Gestión de claves.		
						18.1.5 Regulación de los controles criptográficos.		
						18.1.3 Protección de los registros de la organización.		

ISO 20000								
Gestion de suministradores	Gestion de suministradores			Gestion de la continuidad y disponibilida del servicio	Gestion de suministradores		Gestion de la continuidad y disponibilida del servicio	
				Gestion del Incidente			Gestion del Incidente	
COBIT 5								
APO13: gestión de la seguridad	APO13: gestión de la seguridad		APO13: gestión de la seguridad	APO13: gestión de la seguridad	APO13: gestión de la seguridad	APO13: gestión de la seguridad	APO13: gestión de la seguridad	APO13: gestión de la seguridad
DSS05 Administrar los Servicios de Seguridad	DSS05 Administrar los Servicios de Seguridad		DSS05 Administrar los Servicios de Seguridad	DSS05 Administrar los Servicios de Seguridad	DSS05 Administrar los Servicios de Seguridad	DSS05 Administrar los Servicios de Seguridad	DSS05 Administrar los Servicios de Seguridad	DSS05 Administrar los Servicios de Seguridad
BAI10 Administrar la Configuración						BAI10 Administrar la Configuración		MEA02 Monitorear, Evaluar y Valorar el Sistema de Control Interno
HIPPA								
164.310 (b) USO: uso de la estación de trabajo.	164.312 (e) (1): Seguridad de transmisión - Controles de integridad	164.312 (e) (1): Seguridad de transmisión - Encriptación	164.308 (a) (1): Proceso de gestión de la seguridad - Proceso de gestión de seguridad.	164.310 (b) USO: uso de la estación de trabajo.		164.310 (b) USO: uso de la estación de trabajo.	164.308 (a) (5): Conocimiento de seguridad y capacitación - Protección contra software malicioso	
164.310 C Seguridad: seguridad en la estación de trabajo.			• 164.308 (a) (5): Conciencia y capacitación en seguridad	164.310 C Seguridad: seguridad en la estación de trabajo.		164.310 C Seguridad: seguridad en la estación de trabajo.	164.310 (d) (1): Dispositivos y controles de medios - Responsabilidad	
						164.308 (a) (7): Plan de Contingencia - Plan de Respaldo de Datos	164.310 (b): Uso de estación de trabajo	
						164.308 (a) (7): Plan de Contingencia - Plan de Recuperación de Desastres	164.310 (c): Seguridad de la estación de trabajo	
						164.308 (a) (7): Plan de contingencia - Procedimiento de prueba y revisión		
						164.310 (d) (1): Controles de dispositivos y medios - Copia de seguridad y almacenamiento de datos		
						164.308 (a) (4): Gestión del acceso a la información - Aislamiento de la función del centro de información sanitaria		
						164.310 (d) (1): Dispositivos y controles de medios - Responsabilidad		
						164.312 (a) (1): Control de acceso: cifrado y descifrado		
						164.312 (e) (1): Seguridad de transmisión - Controles de integridad		
						164.312 (e) (1): Seguridad de transmisión - Encriptación		

				ISO 27799				
		7.5.1.2 Cribado Screening Además de seguir la guía dada por ISO / IEC 27002, todas las organizaciones cuyo personal, contratistas o voluntarios procesen (o se espera que procesen) información personal de salud deben, como mínimo, verificar la identidad, dirección actual y empleo previo de dicho personal , contratistas y voluntarios en el momento de las solicitudes de empleo.				7.7.5 Copia de seguridad de información de salud Además de seguir las instrucciones proporcionadas por ISO / IEC 27002, las organizaciones que procesan información de salud personal deben hacer una copia de seguridad de toda la información de salud personal y almacenarla en un entorno físicamente seguro para garantizar su disponibilidad futura."	7.7.4 Protección contra código malicioso y móvil	
						7.6 Seguridad física y ambiental 7.6.1 Áreas seguras 7.6.1.1 Perímetro de seguridad física Las organizaciones que procesan información de salud personal deben usar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información que respaldan dichas aplicaciones de salud. Estas áreas seguras deben estar protegidas por controles de entrada apropiados para garantizar que solo el personal autorizado tenga acceso.	7.7.4.1 Controles contra código malicioso	
						7.8 Control de acceso 7.8.1 Requisitos para el control de acceso en salud 7.8.1.1 General Las organizaciones que procesan información personal de salud deberán controlar el acceso a dicha información. En general, los usuarios de los sistemas de información de salud solo deben acceder a la información de salud personal: a) cuando existe una relación de asistencia sanitaria entre el usuario y el sujeto de los datos (el sujeto de la atención cuya información de salud personal se está accediendo); b) cuando el usuario lleva a cabo una actividad en nombre del interesado; c) cuando hay una necesidad de datos específicos para apoyar esta actividad.	Además de seguir las pautas proporcionadas por ISO / IEC 27002, las organizaciones que procesan información de salud personal deberán implementar controles de prevención, detección y respuesta para protegerse contra software malicioso e implementarán una capacitación apropiada para la conciencia del usuario	
						7.8.1.2 Política de control de acceso Las organizaciones que procesan información de salud personal deben tener una política de control de acceso que rija el acceso a estos datos. La política de control de acceso de la organización debe establecerse sobre la base de funciones predefinidas con autoridades asociadas que sean coherentes con las funciones de esa función, pero que se limiten a ellas. La política de control de acceso, como componente del marco de política de seguridad de la información descrito en 7.2.1, debe reflejar requisitos profesionales, éticos, legales y relacionados con el cuidado y debe tener en cuenta las tareas realizadas por los profesionales de la salud y la tarea. flujo de trabajo		
						7.8.2 Gestión de acceso de usuario 7.8.2.1 Registro de usuario El acceso a los sistemas de información de salud que procesan información de salud personal estará sujeto a un proceso formal de registro de usuario. Los procedimientos de registro del usuario deben garantizar que el nivel de autenticación requerido de la identidad del usuario reclamado sea coherente con los niveles de acceso que estarán disponibles para el usuario. Los detalles de registro del usuario se revisarán periódicamente para garantizar que estén completos, sean precisos y que el acceso sea necesario.		
						7.8.5.1 Restricción de acceso a la información Los sistemas de información sanitaria que procesan la información personal de salud deben autenticar a los usuarios y deben hacerlo mediante autenticación que implique al menos dos factores.		
						7.9.2.1 Temas de cuidado de identificación única Los sistemas de información sanitaria que procesan la información personal de salud deberán: a) asegurar que cada sujeto de cuidado pueda identificarse de manera única dentro del sistema; b) ser capaz de fusionar registros duplicados o múltiples si se determina que múltiples registros para el mismo tema de cuidado se han creado involuntariamente o durante una emergencia médica		
						7.9.2.5 Validación de datos de salida Los sistemas de información de salud que procesan información de salud personal deberán proporcionar información de identificación personal para ayudar a los profesionales de la salud a confirmar que el registro de salud electrónico recuperado coincide con el tema de la atención bajo tratamiento.		
				ITIL				
						Gestion de la continuidad y servicios TI		

NIST 800-53 REVISION 5								
AT-1: Política y procedimientos de sensibilización y capacitación en materia de seguridad	AC-18: Acceso inalámbrico	IA-7: Autenticación del Módulo Criptográfico	AU-3: contenido de los registros de auditoría	CA-2: evaluaciones de seguridad	SA-13: Confiabilidad	AC-23: Protección de minería de datos	CA-7: Monitoreo continuo	CA-2: evaluaciones de seguridad
AT-2: Entrenamiento de Conciencia de Seguridad	AC-19: Control de acceso para dispositivos móviles	SC-12: Establecimiento y gestión de claves criptográficas	AU-5: Respuesta a las fallas en el procesamiento de la auditoría	CA-7: Monitoreo continuo	SA-15: Proceso de desarrollo, estándares y herramientas	AU-2: Eventos de auditoría	SC-39: Aislamiento de proceso	CA-5: Plan de Acción e Hitos
AT-3: entrenamiento de seguridad basado en roles	CA-3: Interconexiones del sistema	SC-13: Protección criptográfica	AU-6: revisión de auditoría, análisis e informes	RA-5: Escaneo de vulnerabilidades	SA-17: Arquitectura y diseño de seguridad del desarrollador	AU-3: contenido de los registros de auditoría	SC-44: Cámaras de detonación	CA-6: Autorización de seguridad
AT-4: Registros de entrenamiento de seguridad	CA-7: Monitoreo continuo	SC-17: Certificados de infraestructura de clave pública	AU-7: Reducción de Auditoría y Generación de Informes	SC-34: Programas Ejecutables No Modificables	SA-20: Desarrollo personalizado de componentes críticos	AU-4: Capacidad de almacenamiento de auditoría	SI-3: Protección de código malicioso	CA-8: Pruebas de penetración
SA-11: Evaluación y evaluación de seguridad del desarrollador	CM-2: Configuración de línea de base		AU-8: sello de tiempo	SI-4: Monitoreo del sistema de información	SA-21: Evaluación del desarrollador	AU-5: Respuesta a las fallas en el procesamiento de la auditoría	SI-4: Monitoreo del sistema de información	RA-6: Encuesta de Contramedidas de Vigilancia Técnica
SA-16: Entrenamiento proporcionado por desarrollador	IA-3: identificación y autenticación del dispositivo		AU-11: retención de registro de auditoría	SI-7: programas ejecutables de integridad de software, firmware e información	SC-39: Aislamiento de proceso	AU-6: revisión de auditoría, análisis e informes	SI-5: Alertas, advertencias y directivas de seguridad	SI-6: Verificación de la función de seguridad
PM-13: Fuerza de trabajo de seguridad de la información	SC-8: Confidencialidad e integridad de la transmisión		AU-12: Generación de Auditoría	SI-2: Remediación de fallas	SI-10: Validación de entrada de información	AU-7: Generación de informes y reducción de auditorías	SI-7: software, firmware e información Integrit	PM-6: Medidas de seguridad de la información del rendimiento
PM-14: Pruebas, capacitación y monitoreo	SC-17: Certificados de infraestructura de clave pública		AU-9: Protección de la información de auditoría		SI-11: Manejo de errores	AU-8: Sellos de tiempo	SI-8: protección contra correo no deseado	PM-14: Pruebas, capacitación y monitoreo
PM-15: Contactos con grupos de seguridad y asociaciones	SC-40: Protección de enlace inalámbrico				SI-15: filtrado de salida de información	AU-9: Protección de la información de auditoría		
PM-16: Programa de concientización sobre amenazas	SI-4: Monitoreo del sistema de información				SI-16: Protección de memoria	AU-10: No repudiatio		
						AU-11: retención de registro de auditoría		
						AU-12: Generación de Auditoría		
						AU-13: Monitoreo de divulgación de información		
						AU-14: Auditoría de la sesión		
						CA-6: Autorización de seguridad		
						CA-7: Monitoreo continuo		
						IA-10: identificación adaptable y autenticación IA-11 Re-autenticación		
						1A-11: Re-autenticación		
						SI-4: Monitoreo del sistema de información		
						CM-9: Plan de gestión de configuración		
						CM-10: Restricciones de uso de software		
						MP-4: almacenamiento de medios		
						AC-4: Aplicación de flujo de información		
						CA-3: Interconexiones del sistema		
						CM-2: Configuración de línea de base		
						CM-3: Control de cambio de configuración		
						CM-5: Restricciones de acceso para el cambio		
						CM-6: Configuración de configuración		
						CM-8: Inventor de componentes del sistema de información		
						MA-4: Mantenimiento no local		
						SC-24: falla en estado conocido		
						AC-17: acceso remoto		
						AC-20: uso de sistemas de información externos		
						SA-9: Servicios del sistema de información externo		
						SC-7: Protección de límites		
						SC-8: Confidencialidad e integridad de la transmisión		
						AC-3: Control de acceso		
						CA-9: Conexiones internas del sistema		
						IR-9: Respuesta al derrame de información		
						MP-5: Transporte de medios		
						SA-18: resistencia a la manipulación y detección		
						SC-28: Protección de la información en reposo		
						SC-31: Análisis de canal secreto		
						SC-41: Puerto y acceso a dispositivos de E / S		

SALVAGUARDAS ADMINISTRATIVAS								
Gestion de Activos			Gestion de identidades, privelegios y accesos			gestion de incidentes y continuidad del negocio		
Inventario de Hardware	Inventario de Software	Inventario de datos e información	Control de uso y administracion de privelegios	Seguridad y configuracion de Hw y SW	Controles de acceso basados en la necesidad de conocer	Evaluacion y remediacion de la continuidad	Administracion, respuesta y gestion de incidentes	Compromiso de la alta direccion
						ISO 27002: 2013	ISO 27002: 2013	ISO 27002: 2013
ISO 27002: 2013								
8.1.1 Inventario de ACtivos	12.5.1 Instalación del software en sistemas en producción.	7.1.1 Investigación de antecedentes.	9.1.1 Política de control de accesos.	14.2.4 Restricciones a los cambios en los paquetes de software.	9.1.1 Políticas de control de acceso	12.1.2 Gestion de cambios	6.1.3 Contacto con las autoridades.	5.1.1 Conjunto de políticas para la seguridad de la informacion
8.1.4 Devolucion de los activos	12.6.2 Restricciones en la instalación de software.	7.1.2 Términos y condiciones de contratación.	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	9.2.1 Gestion de altas y bajas en el registro de usuarios	12.1.3 Gestion de capacidades	7.2.1 Responsabilidades de gestión.	5.1.2 Revision de las políticas para la seguridad de la informacion
8.2.3 Manipulacion de activos	8.2.3 Manipulacion de activos	8.2.1 Directrices de Clasificacion	9.3.1 Uso de información confidencial para la autenticación.	18.2.3 Comprobación del cumplimiento.	9.2.2 Gestion de los derechos de acceso asignados a usuarios	17.1 Continuidad de la seguridad de la informacion	16.1.2 Notificación de los eventos de seguridad de la información.	6.1.1 Asignacion de responsabilidades para la seguridad de la informacion
11.2.5 Salida de activos fuera de las dependencias de la empresa		8.2.2 Etiquetado y manipulado de la informacion	9.4.1 Restricción del acceso a la información.	12.5.1 Instalación del software en sistemas en producción.	9.2.3 Gestion de los derechos de acceso con privelegios especiales	18.1.4 Protección de datos y privacidad de la información personal.	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	6.1.2 Segregacion de tareas
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.		18.2 Revisiones de la seguridad de la informacion.	9.4.4 Uso de herramientas de administración de sistemas.	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	9.24 Gestion de informacion confidencial de autentiacion de usuarios		16.1.7 Recopilación de evidencias.	6.1.3 Contacto con las autoridades
9.1.2 Control de acceso a las redes y servicios asociados.			9.2.1 Gestión de altas/bajas en el registro de usuarios.	15.1.3 Cadena de suministro en tecnologías de la informacion y comunicaciones	9.2.5 Revision de los derechos de acceso a los usuarios		6.1.2 Segregacion de tareas	6.1.4 Contacto con los grupos de interes especial
13.1.1 Controles de red.			9.2.6 Retirada o adaptación de los derechos de acceso		9.2.6 Retirada o adaptacion de los derechos de acceso			7.1 Antes de la contratacion
			9.4.3 Gestión de contraseñas de usuario.		9.3.1 Uso de información confidencial para la autenticacion			7.3 Cese o cambio de puesto de trabajo
			11.2.8 Equipo informático de usuario desatendido.		9.4.3 Gestion de contraseñas de usuarios			6.1.5 Seguridad para la informacion en la gestion de proyectos
			11.1.2 Controles físicos de entrada		10.1.2 Gestion de Claves			6.2.1 Políticas de uso de dispositivos para la movilidad
			9.4.2 Procedimientos seguros para el inicio de sesion		8.3.1 Gestión de soportes extraíbles.			8.1.2 Propiedad de los activos
			9.4.3 Gestion de contraseñas de usuarios		10.1.1 Política de uso de los controles criptográficos.			7.2.2 Concienciación, educación y capacitación en segur. de la informac.
			10.1.2 Gestion de Claves					
			13.2.1 Políticas y procedimientos de intercambio de información.					
ISO 20000			ISO 20000	ISO 20000	ISO 20000	ISO 20000	ISO 20000	ISO 20000
					Gestion de la seguridad de la informacion	Gestion de la seguridad de la informacion	Gestion del Incidente	Gestion de la continuidad y disponibilida del servicio
							Gestion de la seguridad de la informacion	Gestion de la capacidad
								Gestion de la continuidad y disponibilida del servicio
								Elaboracion de presupuesto y contabilidad de los servicios TI
								Proceso de entrega
								Gestion del nivel de servicio
			Gestion de la seguridad de la informacion	Gestion de la seguridad de la informacion				Generacion de Informes de servicio



ITIL				ITIL	ITIL	ITIL	ITIL	ITIL
Gestión de la configuración y de activos del servicio	Gestión de la configuración y de activos del servicio	Gestión de la seguridad de la información	Gestión de Accesos				Gestión de Incidencias	Ges con serv
								Ges Con
								Ges pro
NIST 800-53				**NIST 800-53**	**NIST 800-53**	**NIST 800-53**	**NIST 800-53**	**NIS**
CA- 7 MONITOREO CONTINUO	CA-7: Monitoreo continuo	PM-5: Inventario del sistema de información	AC-2: Gestión de cuentas	CA-7: Monitoreo continuo	AC-1: Política y procedimientos de control de acceso	Cp-2: Plan De Contingencia	IR-1: Política y procedimientos de respuesta a incidentes	AT- pro de sen y ca en r seg
IA-3: identificación y autenticación del dispositivo	CM-2: Configuración de línea de base	RA-2: categorización de seguridad	AC-6: Privilegio mínimo	CM-2: Configuración de línea de base	AC-2: Gestión de cuentas	Cp-5: Actualización Del Plan De Contingencia	IR-2: Entrenamiento de respuesta a incidentes	AT- Ent de (de S
SI-4: Monitoreo del sistema de información	CM-8: Inventario de componentes del sistema de información	MP-3: Marca de medios	AC-17: acceso remoto	CM-8: Inventario de componentes del sistema de información	AC-3: Control de acceso	Cp-6: Sitio Alternativo De Almacenamiento	IR-3: Prueba de respuesta a incidentes	AT- ent de s bas role

CM-8: Inventario de componentes del sistema de información	CM-10: Restricciones de uso de software		AC-19: Control de acceso para dispositivos móviles	CM-11: Software instalado por el usuario	AC-6: Privilegio mínimo	Cp-8: Servicios De Telecomunicaciones	IR-4: manejo de incidentes	AT-4: Regi de entrenami de seguri
SA-4: Proceso de adquisición	CM-11: Software instalado por el usuario		CA-7: Monitoreo continuo	SA-4: Proceso de adquisición	AC-24: Decisiones de control de acceso	Cp-9: Respaldo Del Sistema De Información	IR-5: Monitoreo de Incidentes	SA-11: Pru de seguri del desarrolla Evaluatio
PM-5: Inventario del sistema de información	SA-4: Proceso de adquisición		IA-4: Gestión de identificadores	SI-4: Monitoreo del sistema de información	CA-7: Monitoreo continuo	Cp-10: Recuperación Y Reconstitución Del Sistema De Información	IR-6: Informes de incidentes	SA-16: Entrenami proporcion por desarrolla
SC-17: Certificados de infraestructura de clave pública	SC-18: Código móvil		IA-5: Gestión del autenticador	CM-3: Control de cambio de configuración	MP-3: Marca de medios	Cp-11: Protocolos De Comunicaciones Alternos	IR-7: Asistencia de respuesta a incidentes	PM-13: Fu de trabajo seguridad informació
	SC-34: programas ejecutables no modificables		SI-4: Monitoreo del sistema de información	CM-5: Restricciones de acceso para el cambio	RA-2: categorización de seguridad	Cp-13: Mecanismos De Seguridad Alternativos	IR-8: Plan de respuesta a incidentes	PM-14: Pruebas, capacitaci monitorec
	SI-4: Monitoreo del sistema de información		AC-3: Control de acceso	CM-6: Configuración de configuración	SC-16: Transmisión de atributos de seguridad	Cp-4: Prueba Del Plan De Contingencia	IR-9: Respuesta al derrame de información	PM-15: Contactos grupos de seguridad asociacion
	PM-5: Inventario del sistema de información		AC-7: intentos fallidos de inicio de sesión	CM-7: Funcionalidad mínima	SI-4: Monitoreo del sistema de información	Ma-2: Mantenimiento Controlado	IR-10: Equipo Integrado de Análisis de	PM-16: Programa concientiz

							Seguridad de la Información	sob ame
PE-18: Ubicación de los componentes del sistema de información			AC-11: Bloqueo de sesión	CM-9: Plan de gestión de configuración		Ma-3: Herramientas De Mantenimiento		
PE-20: Monitoreo y Seguimiento de Activos			AC-12: Terminación de la sesión	MA-4: Mantenimiento no local		Ma-6: Mantenimiento Oportuno		
SC-28: Protección de la información en reposo			IA-10: identificación adaptable y autenticación	RA-5: Escaneo de vulnerabilidades		Pe-6: Monitorización Del Acceso Físico		
SC-8: Confidencialidad e integridad de la transmisión			SC-17: Certificados de infraestructura de clave pública	SC-15: Dispositivos de cómputo colaborativos		Pl-2: Plan De Seguridad Del Sistema		
MP-7-. Uso de los medios			SC-23: Autenticidad de la sesión	SC-34: Programas Ejecutables No Modificables		Pl-3: Actualización Del Plan De Seguridad Del Sistema		
				SI-2: Remediación de fallas		Pm-14: Pruebas, Capacitación Y Seguimiento		
						Sa-11: Pruebas De Seguridad Del Desarrollador Y Evaluación		

Tabla 63. Mapeo de Buenas prácticas

6.3. Anexo C. Pruebas de herramientas

Las herramientas que se probaron son elegidas de acuerdo a las buenas prácticas que proponen en cada fase del APT, los riesgos identificados en cada fase y teniendo en cuenta las veces que más se citaron por los 15 autores que proponen el modelo de Kill Chain, como se aprecia en la tabla 74, ítem 6.3, y se seleccionaron según el grado de efectividad propuesto por la dirección de señales de Australia. Para dichas pruebas se realizó una plantilla para identificar si cumplen con el nivel de efectividad y protección requerido.

Plantilla de pruebas de herramientas

Descripción de la prueba	
Pasos a seguir	
Herramienta	
Resultados esperados	
Efectividad	
Fase del APT a que aplica	

Tabla 64.Plantilla de pruebas
Fuente de elaboración propia

A continuación se observa la tabla 74, que contiene la compilación de todas las herramientas y estrategias propuestas por autores reconocidos en el mundo contra APT.

Tabla 74. Muestra el resumen donde se muestra el ciclo de vida del APT con el modelo Kill Chain y las técnicas de prevención y detección más recomendadas por Autores.

Fase	**Técnicas de Ingeniería Social**	**Riesgos**	**Técnicas de prevención**	**Técnicas de Mitigación**															
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Reconocimiento	Técnicas presenciales no agresivas	Fisgoneo o buscar en la basura	Pruebas de seguridad , políticas de destrucción de documentos	Router Logs, Firewall logs			✓					✓			✓	✓	✓		✓
			Recopile registros de visitantes																
	Pasivas	Escaneo de red	Proteger la red para evitar el reconocimiento de servicios innecesarios	Políticas DROP para firewall															
	Técnicas no presenciales	Rootkit	Actualizaciones de software y parcheo de vulnerabilidades	Antivirus															
		Troyano	Registro de logs, http logs (Análisis)	Autenticación(Análisis de trafico DNS logs malicioso), Análisis de Malware		✓	✓		✓	✓		✓		✓	✓				
	Técnicas agresivas	Robo de Identidad, Chantaje	Políticas de contraseñas seguras y cambio de contraseñas	controles de acceso lógico y físico										✓				✓	
	Pasivas	Perfil de los empleados(Redes Sociales, Sitios Web)	Educación en seguridad									✓	✓	✓	✓		✓	✓	✓

	Técnicas no presencia les	DOS	HIDS	NIDS		✓		✓			✓	✓								
			Prevenir inundaciones (floods) en los protocolos TCP/UDP	Limitar el número de conexiones concurrentes al servidor. Restringir el uso del ancho de banda por aquellos hosts que cometan violaciones.		✓		✓			✓	✓			✓					
		Redes botnets	Filtrado de protocolos innecesarios.	Monitoreo de logs y de las conexiones TCP/UDP que se llevan a cabo en el servidor Limitar la tasa de tráfico proveniente de un único host.		✓		✓			✓	✓					✓			
		Malware	Análisis de navegador	Detección de firmas								✓			✓					✓
				Máquinas de aprendizaje		✓			✓	✓	✓	✓				✓				
				Detección virtual de sambox		✓						✓				✓				
		Sondeo de Servicios	Evaluación de la vulnerabilidad utilizando un equipo azul y Rojo			✓						✓				✓				
		Waltering hole	Correlación de eventos, herramientas y técnicas de generación de gráficos de ataque	Análisis contextual(Enfoques Bayesianos), Análisis Web		✓	✓		✓	✓	✓	✓		✓						

			Revisar la configuración de Routers y Firewalls ACL	Caracterización de reputación (Listas Blancas, MET, SpamFlow)			✓		✓	✓	✓	✓				✓				
	Técnicas no presenciales	Ataque de Ofuscación		Identificación basado en ataques de evasión	✓															
			Segmentación de red, DMZ									✓	✓							
Militarización	Técnicas no presenciales	Archivos infectados	Recolecte archivos y metadatos para análisis futuros	Filtros de reputación (anti spam, antivirus ,Listas blancas, Listas negras y listas de bloque en tiempo real basadas en DNS, ClamAV, SpamAssassin), filtro proxy, Detección de reglas, Políticas basadas en reglas.			✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
		url maliciosa	Identificar e integrar las actividades de evaluación de controles de seguridad																	
		Envió de correo spear phishing	Enumerar vulnerabilidades descubiertas																	
	Técnicas no presenciales	Malware	Analice la línea de tiempo de creación de malware	Análisis de artefactos de malware.			✓	✓	✓	✓	✓	✓	✓			✓			✓
		Exploit	Determinar artefactos de armamento																	

			comunes a las campañas de APT																
		Fuerza Bruta/Diccionario																	
Entrega	Técnicas no presenciales	Phishing	Filtros de ejecución de contenido dinámico					✓	✓	✓	✓	✓	✓	✓			✓	✓	
	Técnicas no presenciales	Botnets	NIPS	NIDS				✓			✓	✓							
	Técnicas no presenciales	Archivos infectados	Computación Segura y confiable basada en controles de software	Analice el medio de entrega									✓	✓				✓	✓
	Técnicas no presenciales		Usuario vigilante								✓								
	Técnicas no presenciales	Troyano	In-line AV					✓			✓			✓			✓		
	Técnicas no presenciales	Malware	Queuing								✓								
			Comprenda la infraestructura ascendente	Consumo de Recursos(para filtrar correo electrónico)			✓	✓	✓	✓			✓	✓				✓	✓

			Entender a los servidores y personas específicos, sus roles y responsabilidades	Random Forests Algorithm				✓	✓										✓
			Recopile registros de correo electrónico y web para la reconstrucción forense	Dataset del email(Vortex-IDS, WEKA),				✓	✓				✓						✓
			Detectar nuevas cargas maliciosas en el punto de entrega	Herramientas de Clasificación de correos				✓					✓	✓					✓
Explotación	Técnicas no presenciales	Rootkit Rootkit	Capacitación de usuarios	HIDS		✓		✓			✓							✓	✓
			Pruebas de correo electrónico para los empleados	Restringir privilegios de administrador															
		Troyano	Actualizaciones(Patch), hardening, Corregir las Vulnerabilidades	Monitorear Alertas del sistema		✓					✓			✓		✓	✓		✓
		Exploits 0 Day	DEP(Prevención de ejecución de datos de Windows)	Bloquear ejecución de programas sin autorización.							✓			✓			✓		✓
		Inyección sql	Capacitación de codificación segura para desarrolladores web	Auditoría del proceso del punto extremo para análisis forense y conocer origen del exploit															
		Malware	Análisis de vulnerabilidades y pruebas de penetración regulares-	Medidas de refuerzo del punto final- Reglas del punto final personalizado para bloquear la ejecución del código shell															
Instalación			Restringir Privilegios	HIDS		✓	✓	✓				✓	✓						✓

	Técnicas no presenciales	Instalación de malware adicional	Entender el malware	Auditoría de proceso de punto final															
				Extrae certificados de cualquier archivo ejecutable firmado															
		Ocultamiento de malware	Chroot jail	Crear nuevas mitigaciones de punto final.							✓							✓	✓
		Backdoor	AV	HIPS				✓			✓			✓	✓				
Comando y control	Técnicas no presenciales	Escalada de Privilegios	Firewall ACL	NIDS		✓	✓	✓	✓	✓	✓	✓					✓	✓	✓
		Propagación																	
		Pivotin																	
		Transferencia no autorizada de datos en resguardo	DLP	Bloquear el canal de comando y control	✓												✓		
			Software para ocultar las pulsaciones de teclado	Análisis completo de malware en la infraestructura de comando y control											✓	✓			✓
			Usar un enfoque de las ErsatzPasswords para mejorar la seguridad de los hashes	Bloquear la categoría proxy, incluidos los dominios "ninguno" o "sin categoría".											✓				✓
			Cifrado de datos																
		Rootkit	NIPS	Intoxicación del receptor de DNS y envenenamiento del servidor de nombres				✓			✓								✓
		Instalación de malware adicional	Tarpi	Red Harden							✓						✓		✓
			DNS redirect	Llevar a cabo investigaciones de código abierto para descubrir nuevas infraestructuras C2 adversas			✓	✓	✓	✓	✓								
			Personalice bloques de protocolos C2 en proxies web																
				Audit log		✓	✓	✓			✓						✓	✓	✓

Acción sobre los objetivos	Técnicas no presencia les	Canal encubierto	Qualility of service(calidad del servicio)	Estrategias de respuesta ante incidentes															
				Plan de comunicaciones															
		Destruir o modificar datos	Honeypot	Capturas de paquetes de red							✓								✓
				Realizar una evaluación de daños															
		Robo de datos	Incluir las lecciones aprendidas	Entender el ataque (Análisis Forense en puntos finales)											✓	✓		✓	✓

1. (Mustafa, 2013), 2. (Luh et al., 2017) , 3. (Giura & Wang, 2013) 4. (Deshmukh, Shelar y Kulkarni , 2014), 5. (Oprea, Li, Yen, Chin, & Alrwais, 2015), 6. (Hutchins, Cloppert, & Amin, n.d.), 7. (Hutchins et al., n.d.), 8. (Moon, Im, Lee, & Park, 2014), 9. (Virvilis & Gritzalis, 2013), 10. (Crowe, W, 2015), 11. (Al-Mohannadi, Mirza, Namanya et al..., 2016), 12. (C h r i s t e n s e n, 2013), 13.(Ioannou, Louvieris, Clewley, & Powell, n.d.)**, 14.**(Bodeau & Graubart, 2013)**, 15.**(Lockheed, 2014)**.**

Tabla 74. Resumen: técnicas de prevención y detección según el ciclo de vida de las amenazas persistentes avanzadas.

Fuente de elaboracón propia.

6.3.1. Pruebas de Filtros web

El proxy solo tendrá una interfaz, es decir que recibe y entrega el tráfico por la misma interfaz. Este funcionará en modo explícito es decir que se debe configurar en el navegador.

La idea es comprobar las siguientes funcionalidades:

- Revisión/prevención de adjuntos en correos personales.

- Descifrado de tráfico SSL.

- Prevención de entrada de malware a la red.

- Reputación Web

- Reputación de archivos. Sandbox, Advanced malware, Protección.

Plantilla de Pruebas de la herramienta

A continuación se aprecian los pasos que se tuvieron en cuenta para realizar las pruebas de la herramienta Web Security Virtual Appliance.

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar - Revisión/prevención de adjuntos en correos Institucionales. -Descifrado de tráfico SSL. - Prevención de entrada de malware a la red. - Reputación Web - Reputación de archivos. Sandbox, Advanced malware, Protección
Pasos a seguir	1. Crear una política de prueba que detecte datos adjuntos
	2. Para que el tráfico cifrado pueda ser escaneado en búsqueda de malware, el proxy debe hacer ruptura de SSL y luego generamos el certificado.
	3. Configurar el proxy para que no se puedan adjuntar y descargar archivos de correo
	4. Crear una política de prevención de entrada de malware a la red con listas de reputación.
	5. Verificar la correcta detención de los incidentes
Herramienta	1. Herramienta Web Security Virtual Appliance.
Resultados esperados	2. Todas las políticas configuradas en la listas de prueba aparecen identificadas en el detalle del incidente y logran su cometido
	3. La detección del incidente se realiza con prontitud en la consola
Efectividad	Excelente
Fase del APT donde aplica	2,3,6 y 7

Tabla 65.Prubas para bloquear adjuntos

Fuente de elaboración propia

Interfaz de acceso

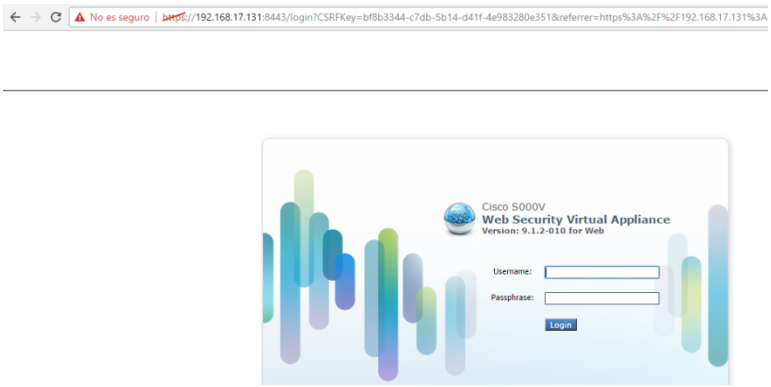


Ilustración 12..Acceso a configuración proxy

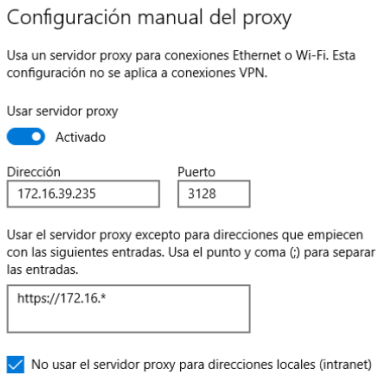


Ilustración 13.Configuración de ruptura de SSL.

Para que el tráfico cifrado pueda ser escaneado en búsqueda de malware, el proxy debe hacer ruptura de SSL y luego generamos el certificado.

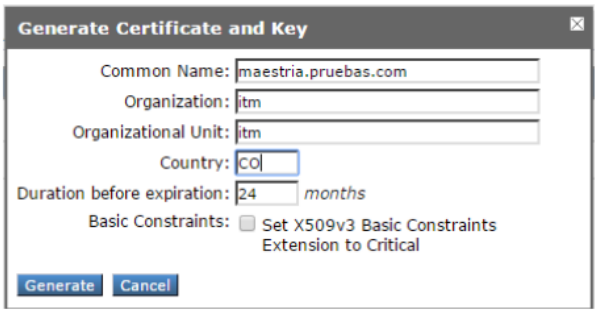


Ilustración 14.Página HTTP cifrada con el certificado emitido

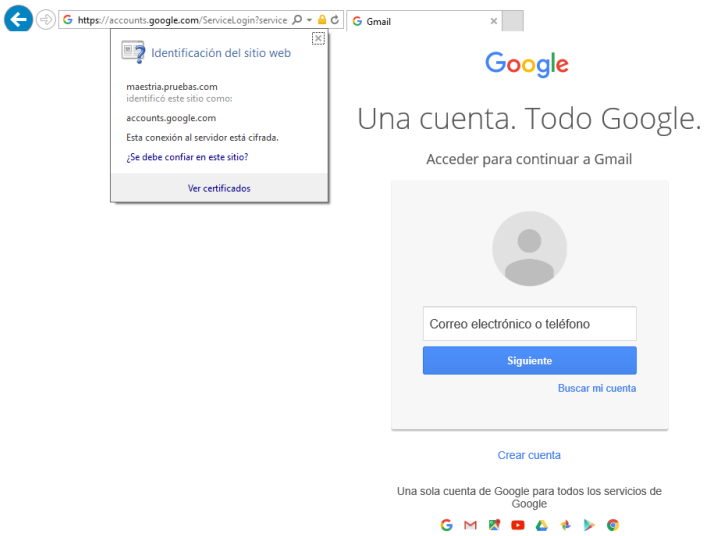


Ilustración 15.Identificación del Sitio Web

A continuación se muestra el tráfico descifrado

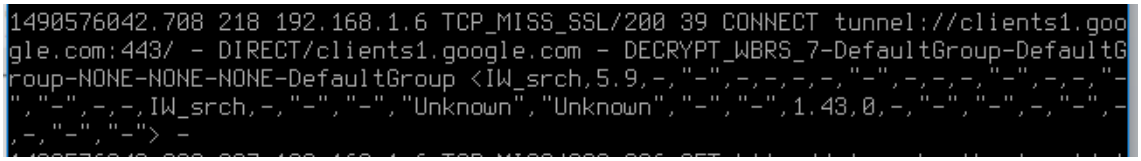


Ilustración 16.Tráfico descifrado

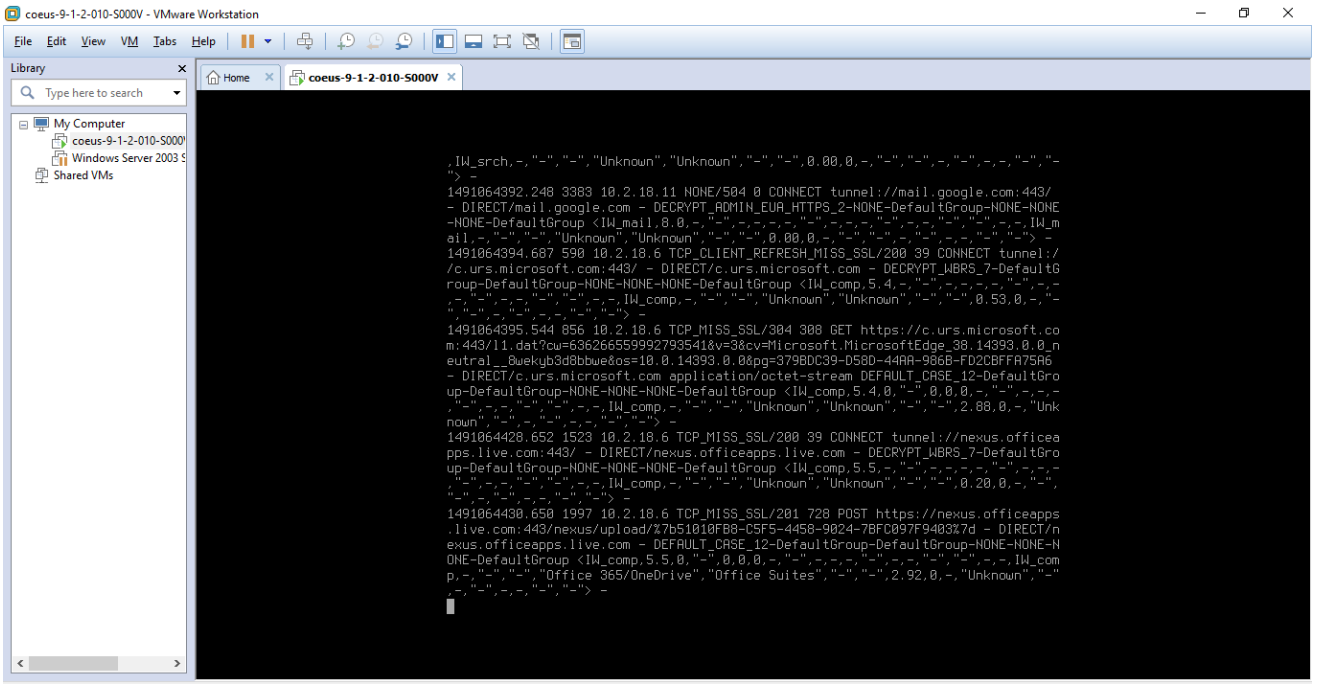
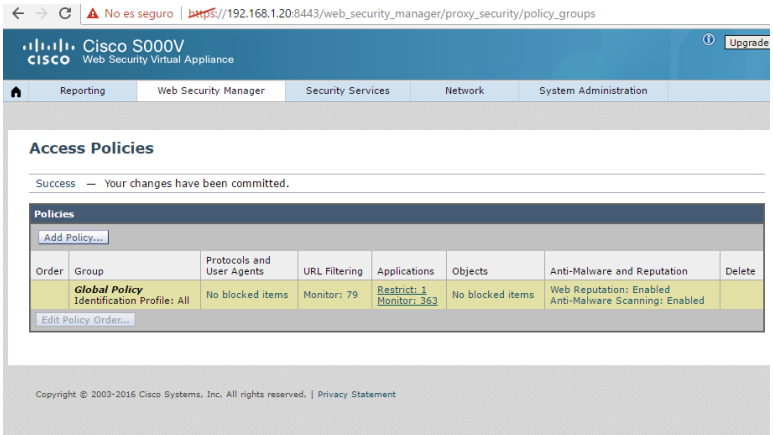


Ilustración 17.tráfico descifrado

Revisión/prevención de adjuntos en correos personales.

Riesgo que se previene: Fuga de información.

Configurar el proxy para que no se puedan adjuntar y descargar archivos de correo.



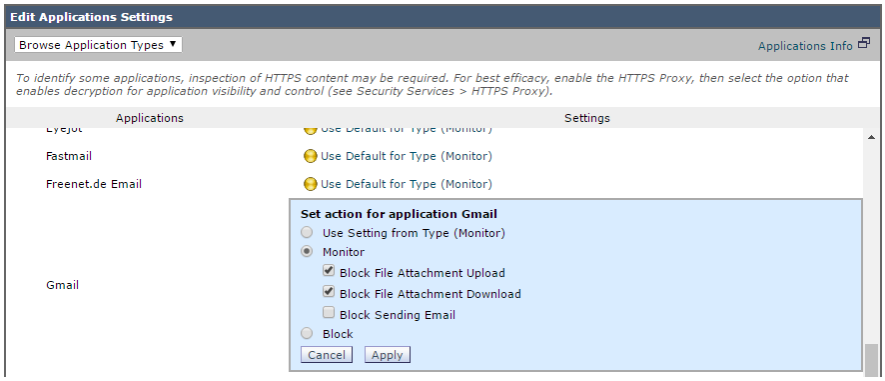


Ilustración 18.Póliticas para datos adjuntos

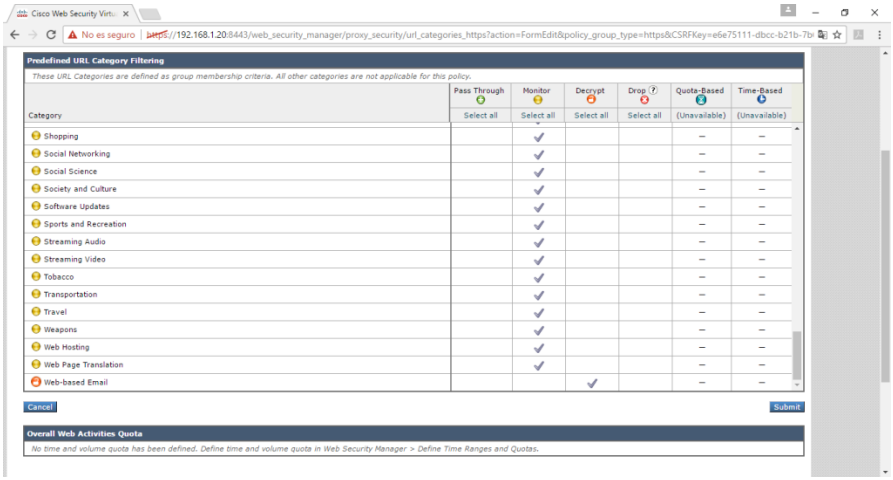


Ilustración 19.Póliticas para datos adjuntos

Resultado se puede observar que bloquea el archivo adjunto

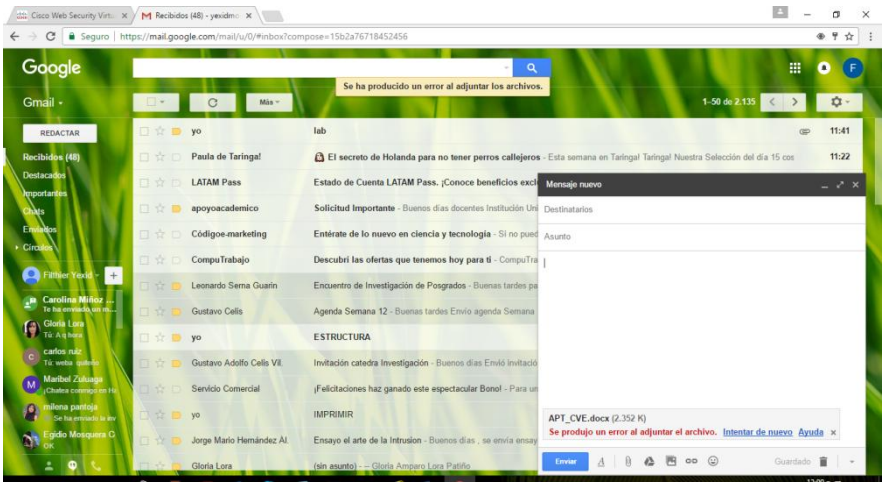


Ilustración 20.Bloqueo de un archivo adjunto

6.3.2. Prevención de entrada de malware a la red con filtros de reputación.

Al tratar de descargar de eicar.com una muestra de malware

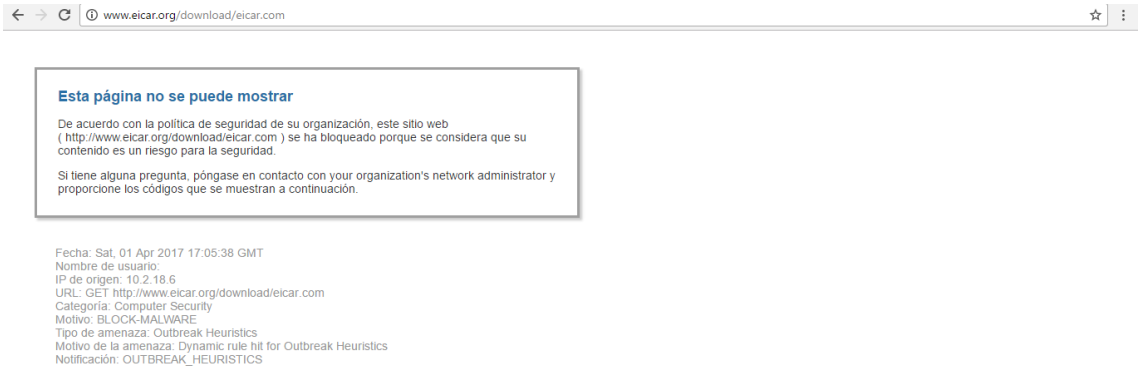


Ilustración 21.Prevención de entrada de malware

6.3.3. Herramientas AntiVirus

En la Herramientas Security services se pueden configurar hasta dos antivirus de los tres disponibles en la herramienta.

Sophos, Webroot, Mcafee. Esta característica disminuye en gran porcentaje la probabilidad de que un intruso descargue malware a la máquina de su víctima. A continuación se muestra la plantilla de pruebas.

Descripción de la prueba	Esta prueba tiene la finalidad bloquear la probabilidad de que un intruso descargue malware a la máquina de su víctima
Pasos a seguir	1. Configurar un antivirus de Security services para establecer protección
	2. Configurar listas negras y análisis dinámico
	2. Ejecutar la herramienta
Herramienta	1. Security services
Resultados esperados	2. Bloquear la descarga del malware
Efectividad	Alto
Fase del APT donde aplica	2,3 y 5

Tabla 66.Pruebas de antivirus

Evidencia

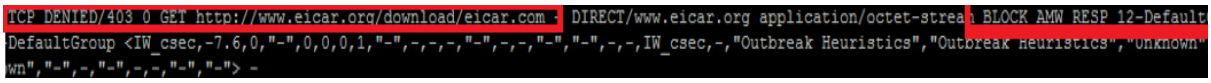


Ilustración 22. Evidencia de bloqueo antivirus

6.3.4. Herramienta Firewall

Se realiza la siguiente configuración para realizar dicha prueba:

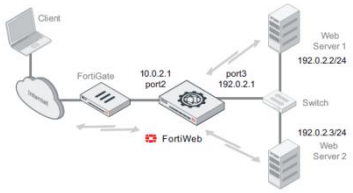


Ilustración 23. Montaje Firewall

Fuente: Fortinet

Para esta herramienta se siguió lo que se estipulo en la plantilla de pruebas que se muestra a continuación.

Pruebas de firewall.

Descripción de la prueba	Esta prueba tiene la finalidad de aplicar la política respectiva y después de esto redireccionar el tráfico al servidor web. El firewall loguea, bloquea o modifica las violaciones de acuerdo a la política que se configure.
Pasos a seguir	1. Crear la política de bloqueo de violaciones
	Configurar las firmas para detectar los diferentes tipos de ataques.
	2. Ejecutar la herramienta
Herramienta	1. Firewall
Resultados esperados	2. Bloquear los intentos de hackeo al servido y registrar los eventos
Efectividad	Alto
Fase del APT donde aplica	6

Tabla 67. Pruebas de firewall

El WAF aplica la política respectiva y después de esto redirecciona el tráfico al servidor web. El firewall loguea, bloquea o modifica las violaciones de acuerdo a la política.

Ambiente de prueba

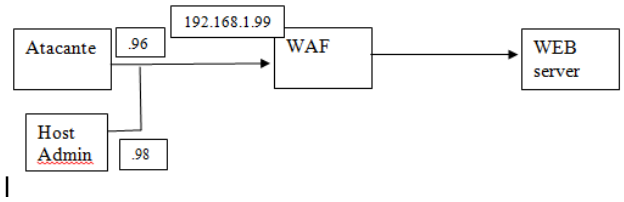


Ilustración 24. Ambiente de prueba

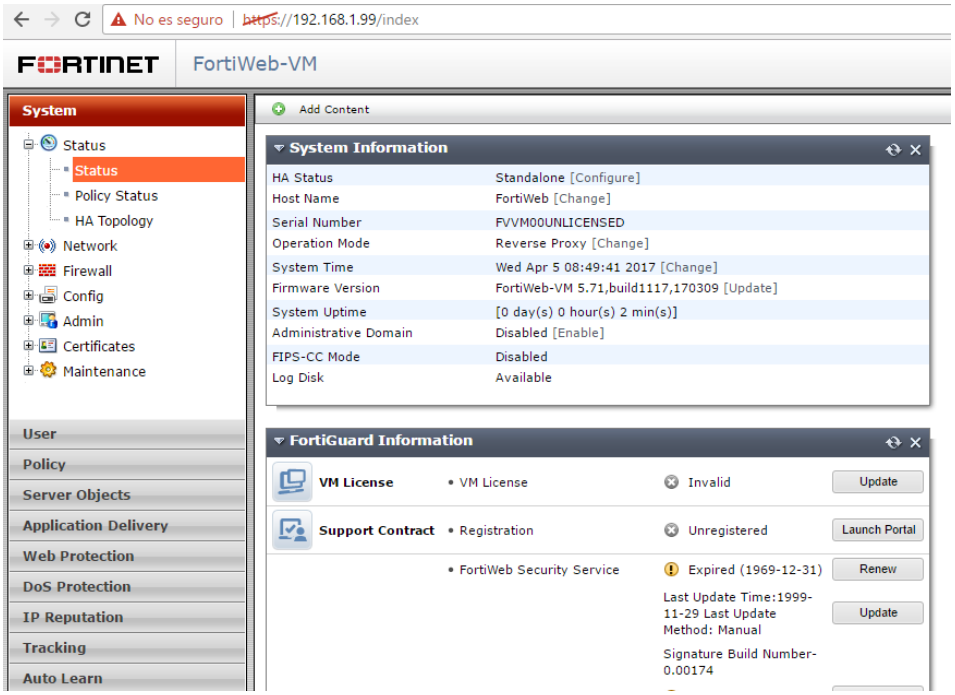


Ilustración 25. Información Fortinet

En la pestaña web protection se pueden ver las firmas para detectar los diferentes tipos de ataques.

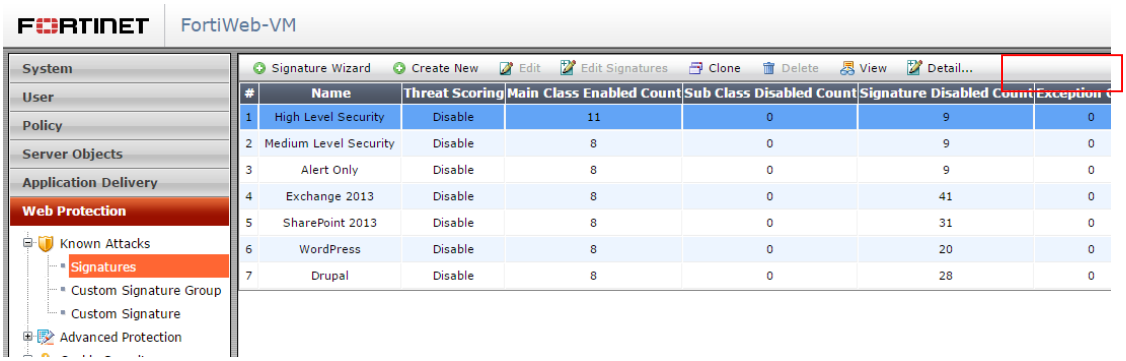


Ilustración 26. Firmas

Ilustración 27.Tipos de ataques

Firma por categoria

ID	Categoría	Descripción	Evento
110000001	Bad Robot	This signature checks whether the request came from a known web scanner . The signature check region: user-agent field in http request header.	User-Agent: webinspect
010000001	Cross Site Scripting	Esta firma impide que los atacantes agreguen funciones de procesamiento de eventos para eventos "mousedown".	Onmousedown
030000001	Sql Injection	Esta firma evita que los atacantes extraigan información sensible de las bases de datos de Oracle utilizando la tabla	select%20count(*)%20from%20sys.user_catalog%20where%20substr(object_name,1,1)='A'

		del sistema "sys.user_catalog".	
04000 0002	SQL Injection (Extended)	Esta firma impide que los atacantes extraigan información de restricciones de base de datos. Esta inyección se puede lograr en URL de solicitud HTTP y argumentos.	(select%20count(*)%20from%20user_constraints%20where%20constraint_type='R')
12001 0003	SQL Injection (Syntax Based Detection)	Inyección booleana basada en la condición	id=1%22+OR+CASE+WHEN+1+%3D+1+THEN+1+ELSE+0+END-
05001 0001	Ataques Genéricos	Esta firma evita que los atacantes acceder a los comandos del sistema operativo. Este ataque se puede lograr de URL de solicitud HTTP y argumentos.	path=%3Bwget%20http://malicious-domain/hack.php
07000 0001	Trojans	Esta regla detecta si hay nombres específicos de cabecera que son utilizados por los caballos de Troya en las cabeceras HTTP. Esta inyección se puede lograr en los nombres de encabezado de solicitud HTTP.	Accept: */* X_File: data.txt

090240001	Known Exploits	Esta firma evita que los atacantes tengan acceso a recursos incrustados a través de la dirección URL con "WebResource.axd" o "ScriptResource.axd". Este ataque se puede lograr en HTTP URL de solicitud.	GET /WebResource.axd?
060020001	Generic Attacks(Extended)	Esta firma evita que los atacantes realizar la inyección de ColdFusion mediante el uso de papeles "ColdFusion" funciones de administrador y etiquetas. Este ataque se puede lograr de URL de solicitud HTTP y argumentos.	name=<CFNEWINTERNALREGISTRY%20ACTION="Set"%20BRANCH="HKEY_LOCAL_MACHINE\Software\Allaire\ColdFusion\CurrentVersion\Server"%20NAME="test"%20TYPE="String"%20VALUE="0">
080030001	Revelación n de Información	Esta firma evita que los atacantes obtener información sensible "PHP". Esta fuga se puede lograr de cuerpo de la respuesta HTTP.	Warning: include(./test.php): failed to open stream: No such file or directory in /usr/local/apache1/htdocs/1.php on line 3 Warning: include(): Failed opening './test.php' for inclusion (include_path='.:/usr/local/php/lib/php') in

			/usr/local/apache1/htdocs/1.php on line 3

Tabla 68. Firmas por categoría

Se Crea un server pool. Esta es la dirección IP del servidor WEB físico. Obviamente esta IP puede variar en cada caso y se debe descubrir cual dirección IP tomó este servidor por medio de DHCP.

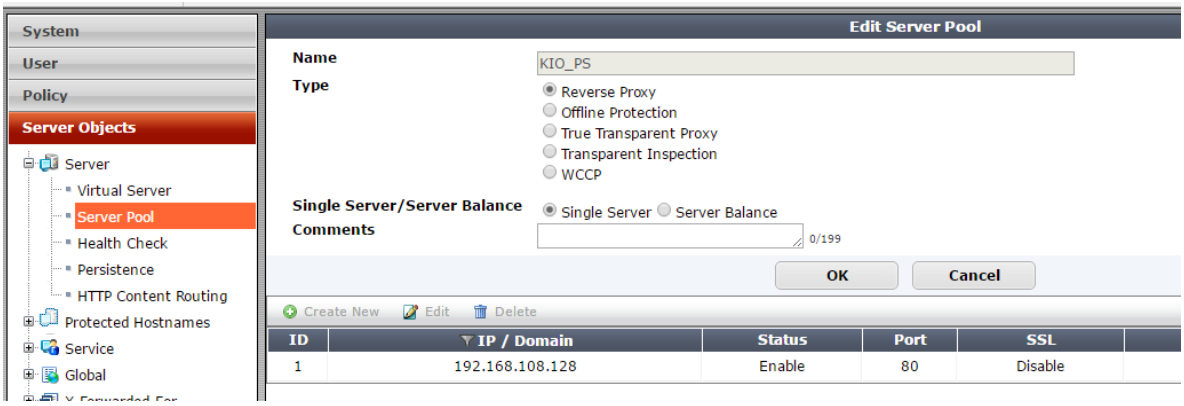


Ilustración 28. Creando Server Pool

Crear una política

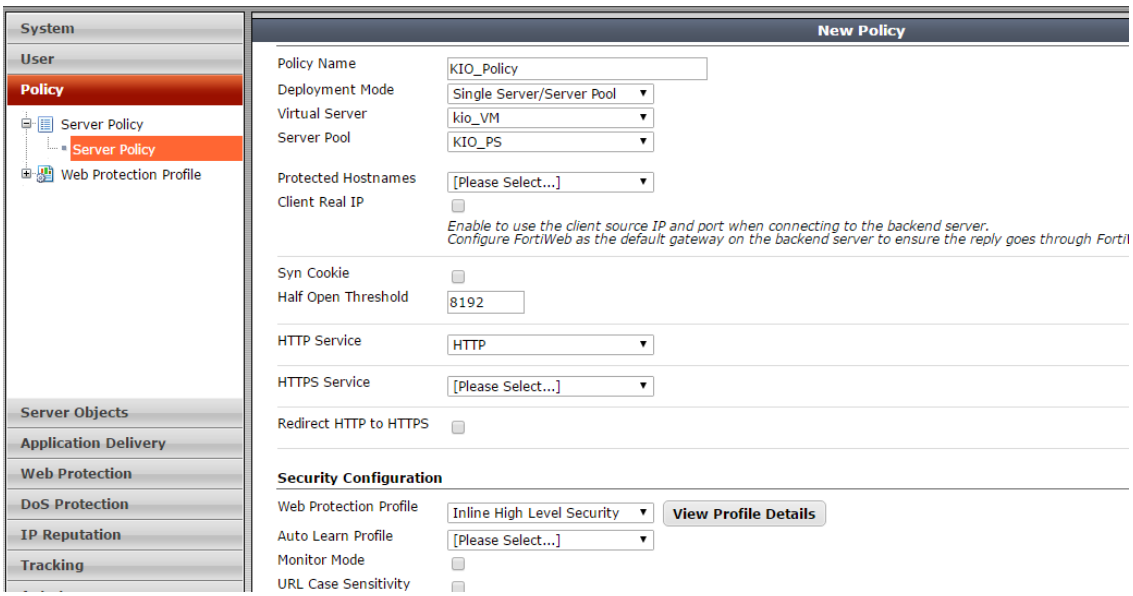


Ilustración 29.Creando Política

Así debería quedar despues de guardar cambios.

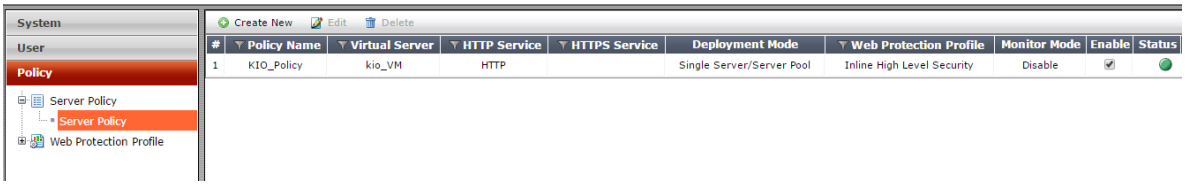


Ilustración 30Politica cumplida

En este momento si la red se encuentra bien configurada ya se debería poder acceder a la página web desde el host o Kali a la máquina kio por medio de la IP virtual que se configuró.

Ilustración 31.Acceso a la web desde el host

Cuando se intente un ataque sobre la anterior página saldrá el siguiente mensaje:

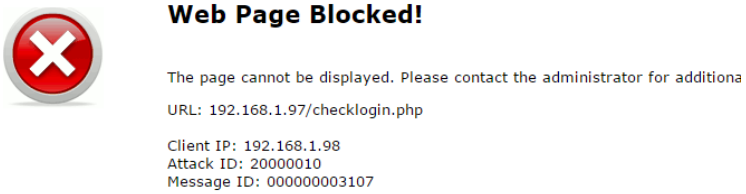


Ilustración 32.Página Bloqueada

Para evitar que el Firewall bloquee los intentos de hackeo de la página se debe cambiar el "Web Protection Profile" a Inline Alert Only.

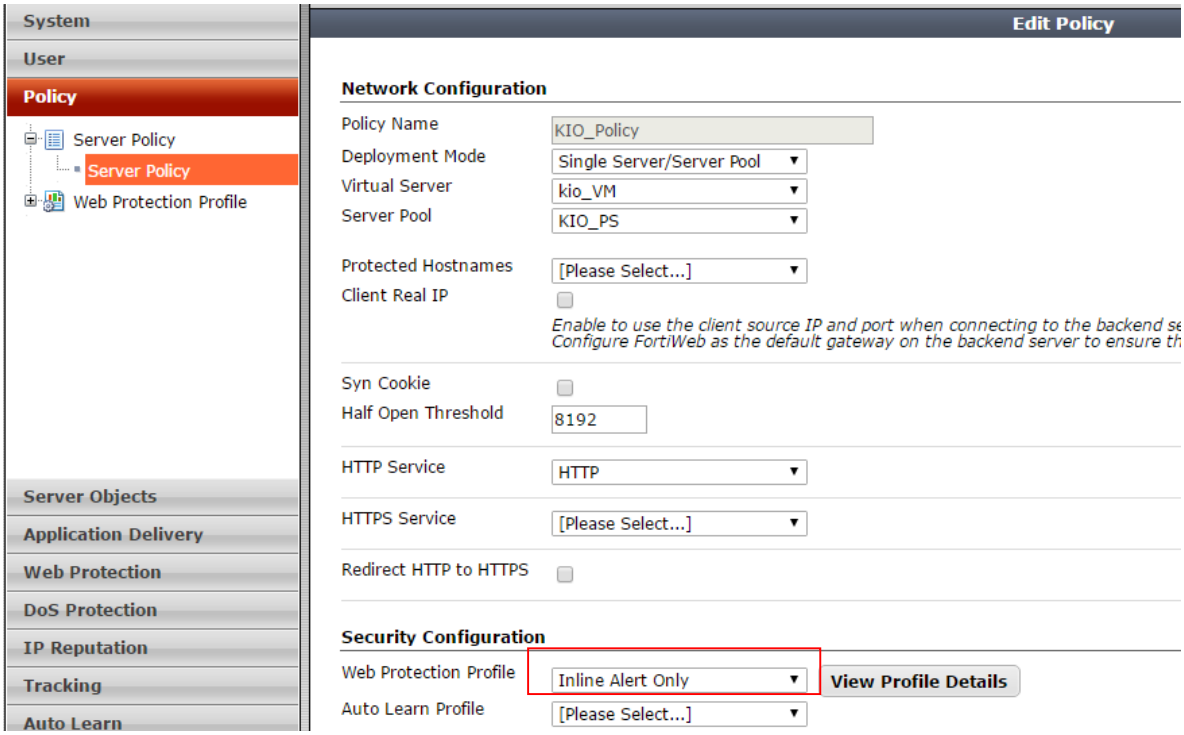


Ilustración 33.Web Protection Profile" a Inline Alert Only

Observar que ahora no se bloquea el intento de hackeo pero este queda registrado en los logs del dispositivo. Ver "matched pattern" en la ilustración 35.

Logs Registrados

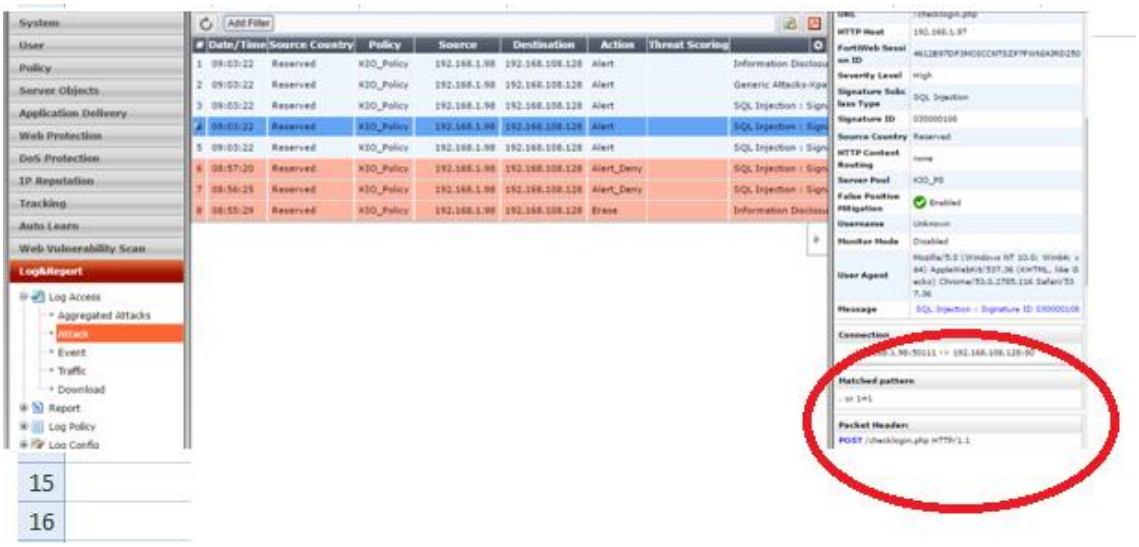


Ilustración 34.Logs del dispositivo

En seguida lo que se pretende es mediante diversas herramientas de hacking tratar de obtener acceso como root al servidor web. En el WAF se irá observando los patrones de ataques lanzados por las diversas herramientas.

Se puede observar que al ejecutar el comando ' or '1'='1'--, dicho comando diseñado paran acceder por el control de acceso de la página web al ejecutase, el fortiweb lo bloquea, debido a que se activa la configuración de la firma para evitar este tipo de ataque de un sql inyection, y al final se puede visualizar en los logs ciertos atributos como son la fecha y hora de inicial del ataque y cuando se termina. Por otra parte se pudo reconocer la dirección ip de la maquina atacante. Con esta información se pueden establecer listas negras y correlación de eventos y establecer filtros DNS.7.2.4

6.3.5. Herramientas de Análisis de los logs y Monitoreo

Se generó un PCAP que contiene tráfico de tres diferentes hosts. También se tiene alertas de los IDS para ayudar a descubrir lo que pasa en una red. En este caso se tiene un PCAP el cual tiene información de un suceso malicioso que infecto las máquinas de una organización en caso se simula que fue una organización de salud. Para dicha prueba se tuvo en cuenta la siguiente plantilla de pruebas. En donde se muestra la efectividad y la fase APT para la cual podría aplicar.

Análisis de Logs

Descripción de la prueba	Esta prueba tiene la finalidad de descubrir lo que pasa en una red
Pasos a seguir	1.Identificar un suceso malicioso que infecto las máquinas de una organización en caso se simula que fue una organización de salud
	2. Identificar los host que fueron infectados
	3. Documentar la familia de malware basados en los indicadores del PCAP observando los logs
Herramienta	1. Herramienta de Análisis de los logs y Monitoreo
Resultados esperados	2. Conocer los equipos infectados y la fecha del suceso
	3. identificación del malware utilizado
Efectividad	Alto
Fase del APT donde aplica	1,3 y 4

Tabla 69. Plantilla de pruebas análisis de logs

Para lo cual se usaron herramientas de análisis de tráfico (Wireshark en nuestro caso), la cual permite analizar protocolos utilizado para realizar análisis

Análisis de Logs.

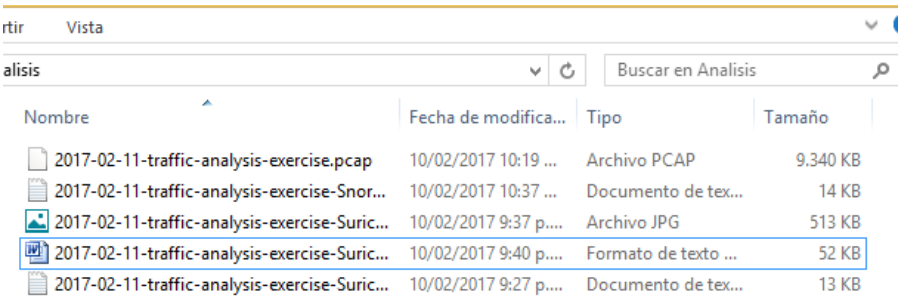


Ilustración 35. Logs del Sistema

Se logró identificar los host que fueron infectados y la fecha de inicio y fin del PCAP

Fecha inicio: 2017-02-11, Hora: 02:57:04.251430

10.3.14.254 10.3.14.135 ICMP 62 Echo (ping) request id=0xd9c5, seq=0/0, ttl=16 (no response found!)

Fin.

Fecha: 2017-02-11

Hora: 03:09:58.606315

Se identificaron las direcciones IP de los tres hosts en el PCAP.

10.3.14.135 `Address: Apple_4c:6b:e1 (00:26:bb:4c:6b:e1)`

`Address: AsustekC_5b:42:1c (14:da:e9:5b:42:1c)`

10.3.14.131 `Address: Dell_18:4c:2a (00:25:64:18:4c:2a)`

Se documenta la MAC address de los tres hosts en el PCAP

00:09:7c:4e:79:b8 `Address: Dell_18:4c:2a (00:25:64:18:4c:2a)`

00:26:bb:4c:6b:e1 `Address: AsustekC_5b:42:1c (14:da:e9:5b:42:1c)`

00:25:64:18:4c:2ª `Address: Apple_4c:6b:e1 (00:26:bb:4c:6b:e1)`

Se determinó el tipo de sistema operativo para cada uno de los tres host en el PCAP

Windows NT10 (10.3.14.131), Windows NT6 (10.3.14.134) y Mac Darwin/14.5.0 (x86_64)(10.3.14.135)

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
537.36
Content-Type: application/x-www-form-urlencoded

Accept: */*
Referer: http://p27dokhpz2n7nvgr.1nmrtq.top/3402-41D8-C680-0091-CCCF/language?t=476376406
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.0.30729; Media Center PC 6.0)

Accept: */*
Accept-Language: en-us
User-Agent: SpotlightNetHelper/917.36 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
```

Ilustración 36. Host Infectados

Se logró determinar cuáles host fueron infectados ver ilustración 37 y 38.

10.3.14.131 y 10.3.14.134

Registro de Logs

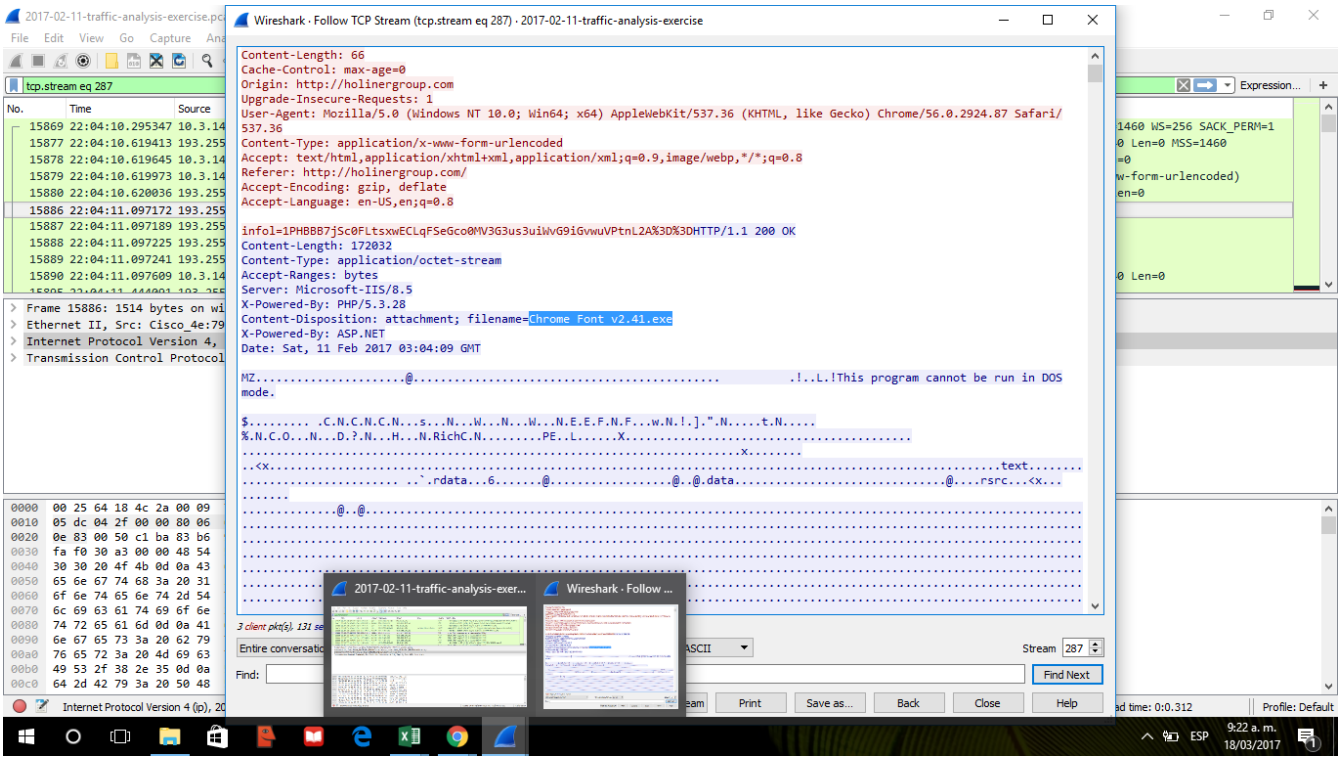


Ilustración 37. Registro de Logs

```
-------
Count:1 Event#3.23810 2017-02-11 03:02:41 UTC
ET DNS Query to a *.top domain - Likely Hostile
10.3.14.134 -> 10.3.14.2
IPVer=4 hlen=5 tos=0 dlen=61 ID=1417 flags=0 offset=0 ttl=128
chksum=1178
Protocol: 17 sport=51734 -> dport=53

len=41 chksum=6660
---------------------------------------------------------------
-------
Count:1 Event#3.23811 2017-02-11 03:02:43 UTC
ET INFO HTTP Request to a *.top domain
10.3.14.134 -> 104.155.4.180
IPVer=4 hlen=5 tos=0 dlen=325 ID=0 flags=0 offset=0 ttl=0 chksum=
13276
Protocol: 6 sport=49249 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=62268 chksum=0
---------------------------------------------------------------
-------
Count:1 Event#3.23812 2017-02-11 03:02:43 UTC
ET POLICY PE EXE or DLL Windows file download
104.155.4.180 -> 10.3.14.134
IPVer=4 hlen=5 tos=0 dlen=1448 ID=0 flags=0 offset=0 ttl=0
chksum=12153
Protocol: 6 sport=80 -> dport=49249

Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=6826 chksum=0
---------------------------------------------------------------
```

Ilustración 38. Eventos del host 10.3.14.134

Se logró documentar la familia de malware basados en los indicadores del PCAP observando los logs de Suricata y se encontró que las familias de los malware encontrados son.

RANSOWARE Cerber.

En las ilustraciones 40 y 41 se muestran los hosts infectados.

```
Count:1 Event#3.23822 2017-02-11 03:02:44 UTC
ET TROJAN Ransomware/Cerber Checkin M3 (4)
10.3.14.134 -> 91.119.56.0
IPVer=4 hlen=5 tos=0 dlen=53 ID=1499 flags=0 offset=0 ttl=128
chksum=35037
Protocol: 17 sport=51735 -> dport=6892

len=33 chksum=17991
---------------------------------------------------------------
-------
Count:1 Event#3.23823 2017-02-11 03:02:44 UTC
ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP
Ping Packet (bit value 16)
10.3.14.134 -> 91.121.56.30
IPVer=4 hlen=5 tos=0 dlen=53 ID=1593 flags=0 offset=0 ttl=128
chksum=34911
Protocol: 17 sport=51735 -> dport=6892

len=33 chksum=17959
---------------------------------------------------------------
-------
Count:1 Event#3.23824 2017-02-11 03:02:50 UTC
ET TROJAN W32/Cerber.Ransomware CnC Checkin M4
10.3.14.134 -> 91.119.56.0
```

Ilustración 39. Host infectados

ET TROJAN Spora Ransomware DNS.

En la siguiente ilustración se muestran los host infectados.

```
Count:1 Event#3.23877 2017-02-11 03:05:47 UTC
ET TROJAN Spora Ransomware DNS Query
10.3.14.131 -> 10.3.14.2
IPVer=4 hlen=5 tos=0 dlen=55 ID=24468 flags=0 offset=0
chksum=43671
Protocol: 17 sport=64890 -> dport=53
```

Ilustración 40.Trojan Spora Ransomware

Por último se documenta la causa raíz para las infecciones notadas en el PCAP y se cree que un usuario visitando un sitio accedió a un link malicio con extensión .exe, y este ejecutó un archivo, el cual contenía un virus de tipo ransomware.

Para la ip 10.3.14.131, se filtra las solicitudes HTTP para esa dirección IP, primero vemos y se verifica el HTTP tráfico y se encuentra el problema raíz.

15879 22:04:10.619973 10.3.14.131 80 193.255.242.61 10.3.14.131 kuzem2.kku.edu.tr HTTP 666 POST /load.php HTTP/1.1 (application/x-www-form-urlencoded)

```
ilename=Chrome Font v2.41.exe
```

Ilustración 41. Archivo ejecutable con malware

Se cree que un usuario desde su correo accedió y ejecuto el malware con extensión .exe.

6.3.6. Herramientas IDS/IPS

Pruebas IDS/IPS

Descripción de la prueba	Esta prueba tiene la finalidad de crear reglas que permitan identificar el tráfico de la red y detectar y bloquear ataques web, realizados desde la herramienta de escaneo de vulnerabilidades.
Pasos a seguir	1. Crear las reglas de bloqueo o de generación de logs.
	2. Construir reglas para detectar los diferentes tipos de ataques.
	2. Ejecutar la herramienta
Herramienta	1. Snort
Resultados esperados	2. Bloquear e identificar de los intentos de hackeo al servido y registrar los eventos
Efectividad	superior
Fase del APT donde aplica	4, 5 y6

Tabla 70. Pruebas ID/IPS

Escenario de pruebas.

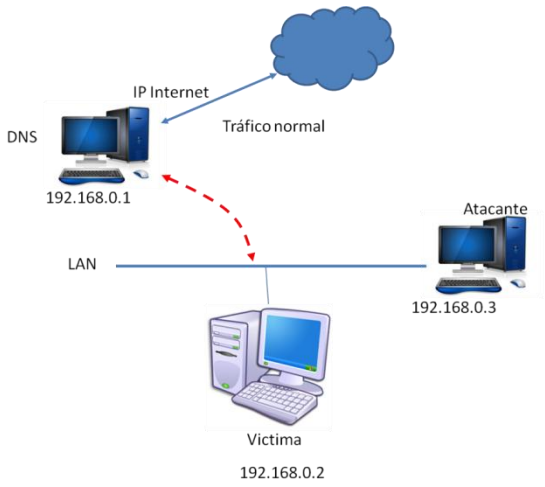


Ilustración 42. Escenario de pruebas

Se realiza la configuración de reglas en snort como se indica en la ilustración 43 y se procede a ejecutar las pruebas de funcionalidad de las reglas configuradas, para ello se ejecuta el comando que se muestra a continuación para analizar el tráfico por la tarjeta de red eth0.

```
root@debian-2:/etc/snort/rules# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:04:a3:ed
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe04:a3ed/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10786 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11528 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:790067 (771.5 KiB)  TX bytes:1428318 (1.3 MiB)
```

Ilustración 43.Configuración de reglas

La ilustración 44 muestra la dirección ip, Mascara y otros elementos configurados en la tarjeta de red. Se ejecuta el comando: para verificar la funcionalidad de las reglas de snort

Ejecución de snort.

```
root@debian-2:/etc/snort/rules# /usr/local/bin/snort -A console -q -c /etc/snort
/snort.conf -i eth0_
```

Ilustración 44.Ejecución de reglas de Snort

La ilustración 45 muestra la ejecución del comando /usr/local/bin/snort -A console -q -c /etc/snort/snort.conf -i eth0.

Desde otra estación en la red se ejecuta ping, se debiera ver por consola lo que llega. Se realiza ping desde la máquina virtual que tiene instalado el sistema operativo windows 2012, y se procede a realizar ping a la ip del Debian 192.168.0.1 y se obtiene una réplica de la maquina atacada como se muestra en la ilustración 46..

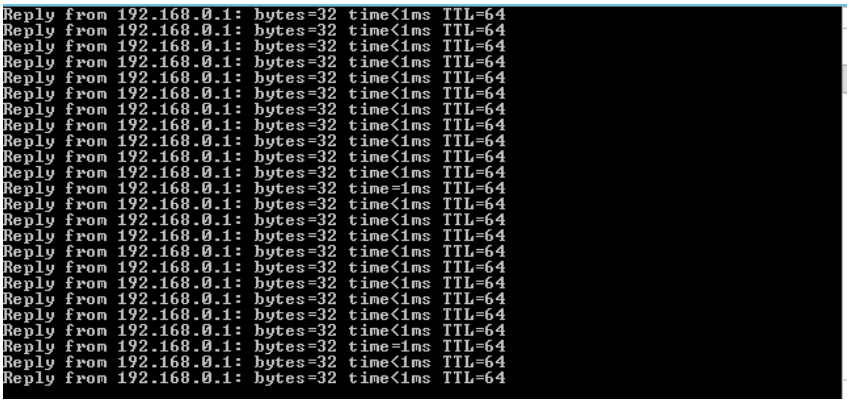


Ilustración 45.Se muestra un ping al servidor debian cuya ip es 192.168.0.1

Nos desplazamos a monitorear el la máquina debian y se visualiza en la imagen, que los eventos se han activado para la dicha regla, identificando la dirección ip de donde se ejecuta el ping, para este caso genera una alerta prioritaria que nos indica que hay un evento en curso ICMP.

Ilustración 46.Alerta de evento sospecho con ICMP

PRUEBA de Acceso HTTP

Modificar el archivo /etc/snort/rules/local.rules e incluir:

alert tcp any -> any 80 (msg:"Prueba para HTTP"; GID:1; sid:10000002; rev:002; classtype:attempted-admin;) o Incluir la siguiente línea en el archivo /etc/snort/sid-msg.map

2 || 10000002 || 002 || http-event || 0 || Prueba de HTTP

En esta prueba se valida que la regla haya quedado bien construida y se prueba que haya navegación a un sitio Web en el servidor, haciendo uso del comando:

sudo snort -T -c /etc/snort/snort.conf -i eth0.

Se ejecuta el comando, y se procede a digitar la dirección ip del Debian 192.168.0.1, en cual muestra en la ilustración 6 que existe respuesta y conexión exitosa haciendo uso de http.

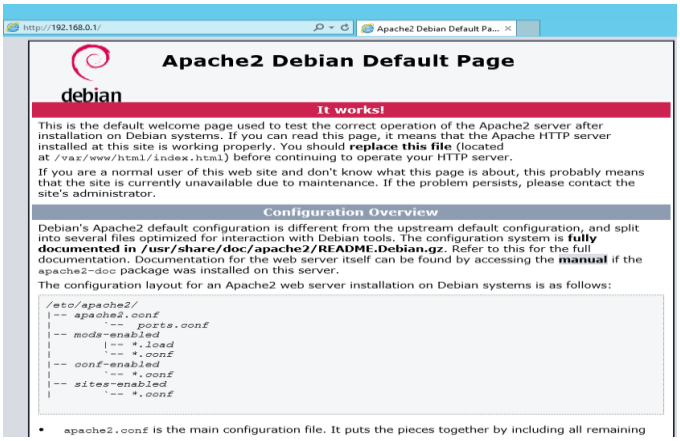


Ilustración 47.conexión al servicio apache en el servidor debian digitando la ip por el navegador web

Luego visualizamos que se ha activado la regla para ataques web configurada en el snort, Además se visualiza la dirección ip del equipo en donde se abrió el navegador, adicionalmente se observa la fecha, la hora en que realizaron dicha conexión.

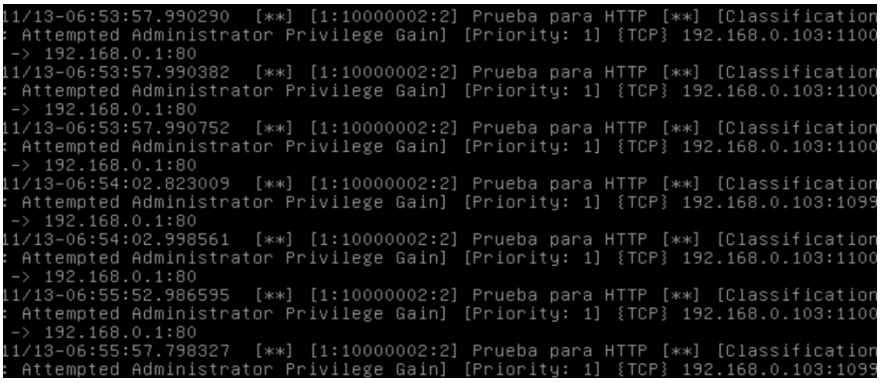


Ilustración 48.Evento generados después de detectar que existe un conexión en su servidor web.

- **7.2.6.1.Construcción De Reglas**

Se construyen y se ponen en funcionamiento las siguientes reglas Alertas/logs:

escaneos de nmap.

Se configura la regla para más adelante realizar el escaneo de puertos, desde la herramienta nmap versión kali linux. En nuestro caso definimos la siguiente regla.

alert tcp any any -> $HOME_NET any (msg: " Escaneo de puertos con nmap"; flags: F; sid:900001;

- **7.2.6.2. La regla para un escaneo de puertos con nmap.**

Luego se procede desde el sistema operativo kali linux a ejecutar el siguiente comando. nmap -sF 192.168.0.1, que se usa para realizar el escaneo de puertos abiertos del servidor Debian como se observa en la siguiente ilustración 49.

Se puede apreciar que con el escaneo realizado se encuentran los puertos 53,80, 111 se encuentran abiertos con sus respectivos servicios y se muestra la dirección mac..

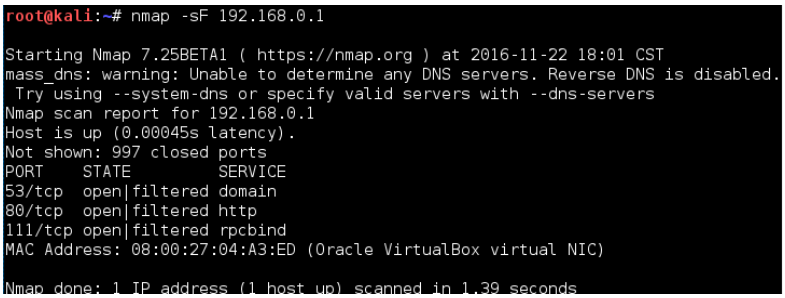


Ilustración 49.Muestra el escaneo de puerto de la maquina 192.168.0.1

En la herramienta de snort se activa un evento, en este caso es la regla configurada para alertar sobre escaneos de puertos, como también se puede apreciar el registro del monitoreo, el cual indica la dirección ip de donde se ha ejecutado la solicitud de escaneo como se muestra a continuación.

Ilustración 50.Muestra eventos generados en Snort sobre escaneo de puertos con nmap

Ataques Syn Flood Con Hping

Se procede a configurar la regla en snort de la siguiente manera.

alert tcp any any -> $HOME_NET any $HOME_NET (msg:" SYN ";flags:S; reference:arachnids,28;classtype:attempted-recon; sid:628;rev:1;)

Se realiza el ataque solicitado como se muestra en la ilustración 10

Ilustración 51.Muestra ataque SYN flood con hping

Luego se procede a ejecutar el comando nmap -Ss 192.168.0.1, y hapin 3 desde el sistema operativo kali -linux como se muestra en la ilustración 11 y 12 respectivamente para verificar el funcionamiento con estos tipos de ataques.

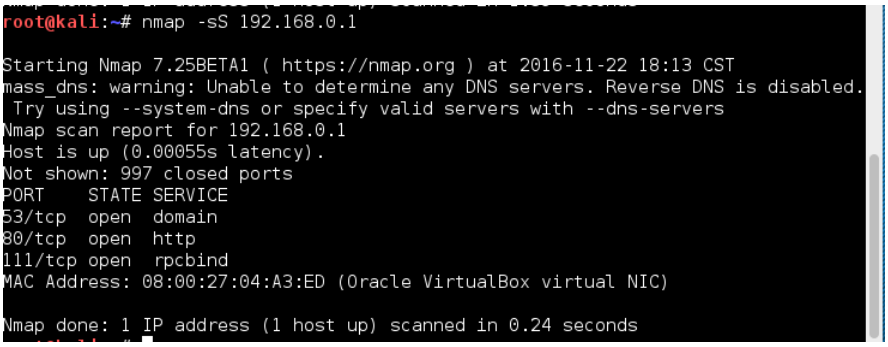


Ilustración 52.Muestra eventos generados con ataque con comando nmap -Ss 192.168.0.1.

Se identifica en la consola de snort que se activa la regla configurada para detectar dicho ataque. Se identifica la dirección ip de donde ejecutaron el comando, al tiempo que se puede apreciar que el comando hping3 inunda al puerto 80 con ips generadas de forma aleatorias.

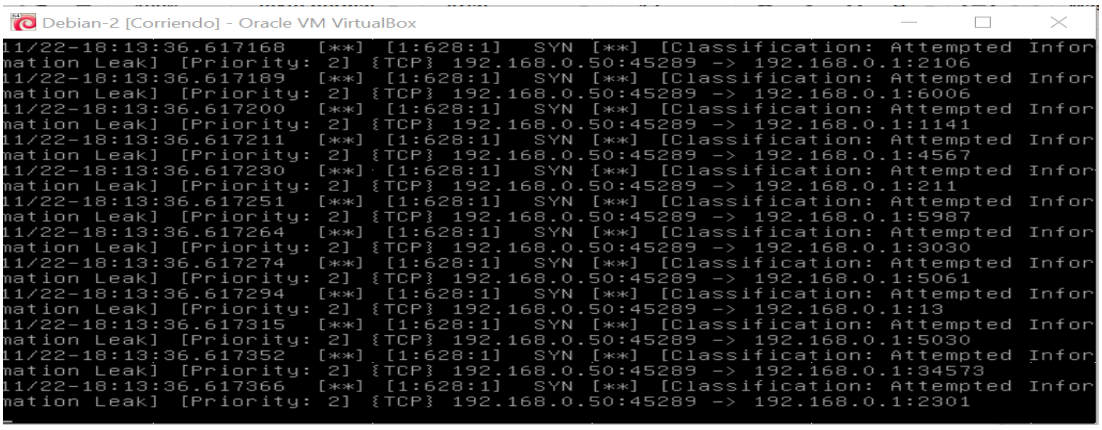


Ilustración 53.Muestra evento generado al ejecutar ataque SNY.

Se ejecuta desde debian el comando tcpdump –x –r –n /var/log/snort/snort.log para monitorear los logs y se muestra efectivamente los registros que con las reglas se detectaron anteriormente.

Comando tcpdump monitoreo de logs

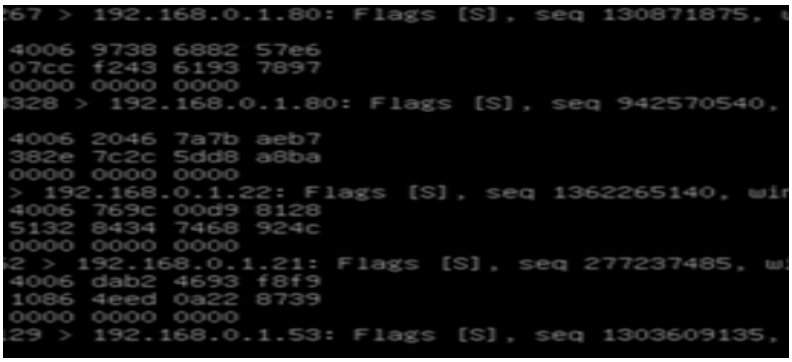


Ilustración 54.Muestra los logs generados a partir de tcpdump –x –r –n /var/log/snort/snort.log

Ataques snmp

Creamos una regla en el debian para la detección de snmp como se muestra a continuación para generar eventos cuando se haga una ataque haciendo uso del protocolo udp. Para este ejercicio se configuró la siguiente regla:

alert udp any any -> $HOME_NET 161 (msg: “ Ataque SNMP; sid:9000014”;)

En la herramienta kali linux se ejecuta el siguiente comando.

snmpwalk -v 2c -c ataque 192.168.0.1

```
root@kali:~# snmpwalk -v 2c -c ataque 192.168.0.1
```

Ilustración 55.Muestra un ataque snmp a la máquina debian.

Automáticamente se activa la regla para detectar ataques snmp, después de haber ejecutado el comando en la máquina kali linux. En la anterior ilustración se visualiza la dirección ip de la máquina atacante, cuando snort detecta un ataque y genera una alerta.

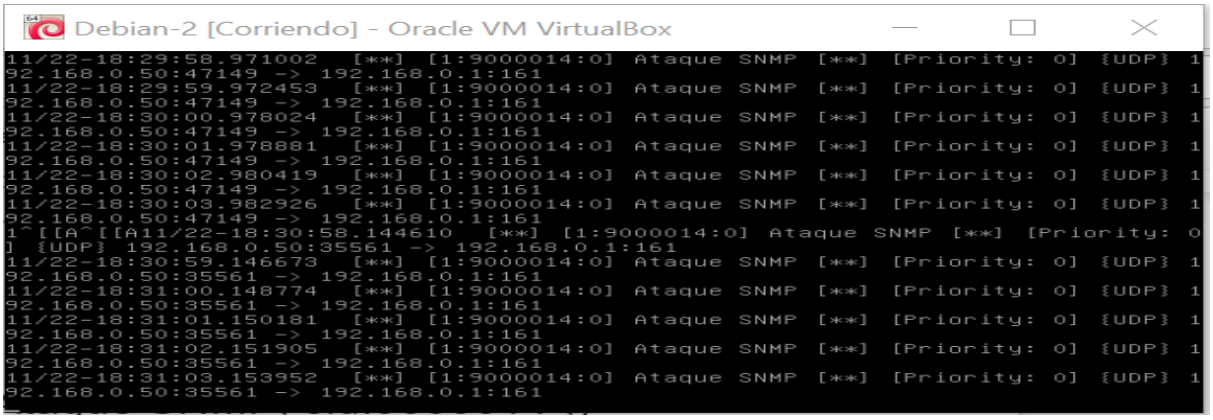


Ilustración 56.Muestra eventos generados en snort y ataque SNMP en progreso.

Adicionalmente es posible configurar otras reglas para detectar ataques SNMP, en la herramienta snort. Como las que se enuncian a continuación.

alert tcp any any -> $HOME_NET 705 (msg:"SNMP AgentX/tcp request"; flow:stateless; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve,2002-0012; reference:cve,2002-0013; classtype:attempted-recon; sid:1421; rev:11;)

alert udp any any -> $HOME_NET 161 (msg:"SNMP missing community string attempt"; content:"|04 00|"; depth:15; offset:5; reference:bugtraq,2112; reference:cve,1999-0517; classtype:misc-attack; sid:1893; rev:4;)

alert udp any any -> $HOME_NET 161 (msg:"SNMP null community string attempt"; content:"|04 01 00|"; depth:15; offset:5; reference:bugtraq,2112; reference:bugtraq,8974; reference:cve,1999-0517; classtype:misc-attack; sid:1892; rev:6;)

Fragmentación Por Icmp

A continuación se muestra una regla para detectar ataques de fragmentación ICMP y se configura en la herramienta snort.

alert icmp any any -> any any (msg:" Detectando ping fragmentado "; dsize: >800; sid:9000018;)

Se ejecuta el comando ping –l 9000 192.168.0.1 en el sistema operativo windows 2012, para activar la regla configurada.

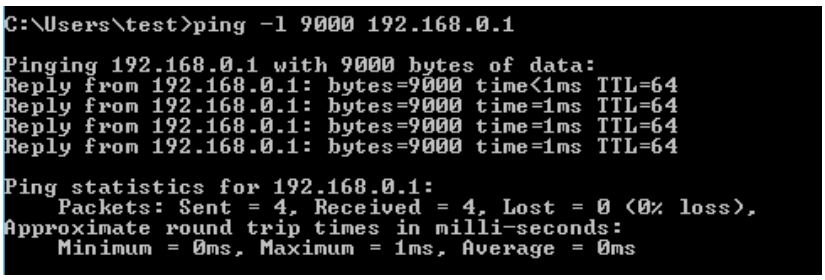


Ilustración 57.Muestra la ejecuciòn de un ataque pin fragmentado, la cual indica que hay respuesta de la máquina atacada.

Después de haber ejecutado el ataque se procede a capturar los datos que se generan en la herramienta snort en la máquina debian como se indica en la siguiente ilustración.

Ilustración 58.Muestra la detección de un ping fragmentado mediante ICMP.

Luego se ejecuta el comando ping -s 9000 192.168.0.1, desde el sistema operativo kali linux hacia la máquina debian.

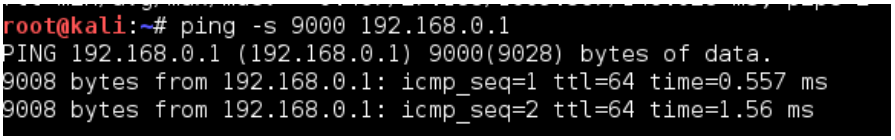


Ilustración 59.Muestra que se realiza conexion exitosa con ICMP al ejecutar de ping -s 9000 192.168.0.1

Automáticamente se pueda apreciar que se generan eventos que indican la detección de un ping fragmento con ICMP, como se muestra en la siguiente captura captura de datos del monitoreo de la herramienta snort.

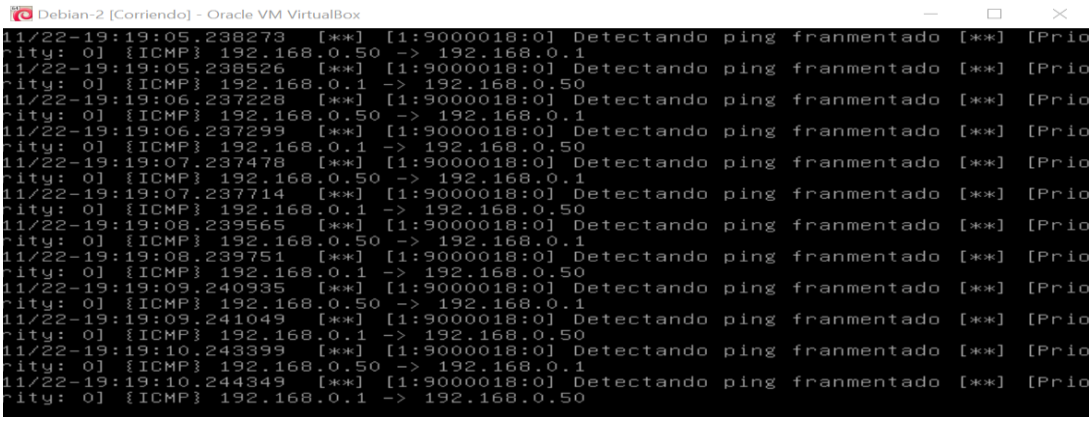


Ilustración 60.Muestra la detección de un ping fragmentado a través de ICMP.

para proteger los servicios que no estén protegidos por el Firewall.

Se generan reglas personalizadas y se hace uso de otras reglas ya configuradas en snort para servicios como MySQL. Entonces accedemos a reglas de Mysql y se configura la siguiente regla que permite saber cuándo existe una conexión a mysql desde una máquina no autorizada.

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:" Conexion MYSQL"; flow:to_server,established; content:"|01|"; distance:3; within:1; content:"root|00|"; nocase; distance:5; within:5; classtype:protocol-command-decode; sid:3456; rev:1;)

También es posible usar esta regla para alertar que se estableció una conexión a la base de datos.

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL show databases attempt"; flow:to_server,established; content:"|0F 00 00 00 03|show databases"; classtype:protocol-command-decode; sid:1776; rev:2;)

Por último para realizar la validación de las reglas mencionadas, se debe tener acceso desde un cliente de mysq como se muestra en la ilustración 62.

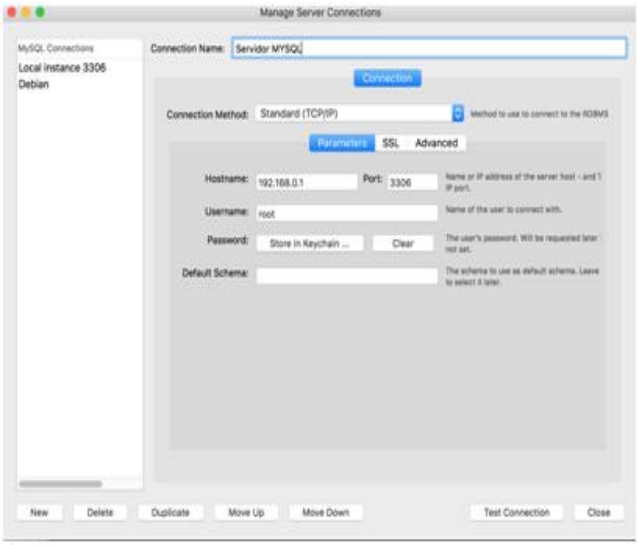


Ilustración 61.Muestra conexión a servidor Mysql remotamente

Se generan eventos en la máquina debian que indican que se realizó una conexión a el servidor mysql, esta máquina tiene configurada la regla de snort para detectar una conexión a Mysql como se muestra a continuación.

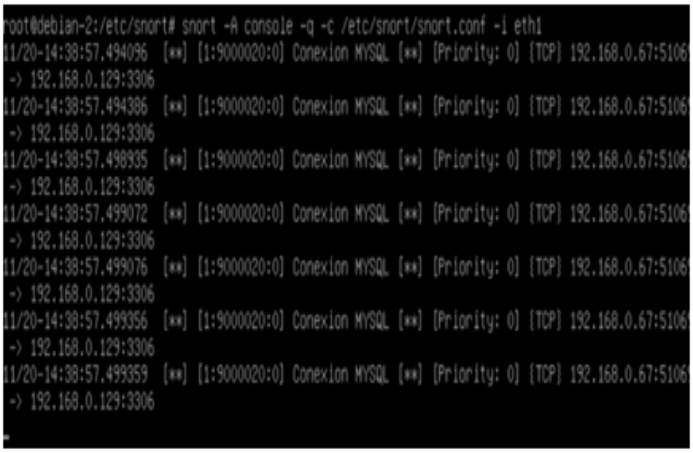


Ilustración 62.Muestra detección de conexión a Mysql.

- **7.2.6.3.IPS**

La siguiente ilustración muestra un IPS que actúa como router.

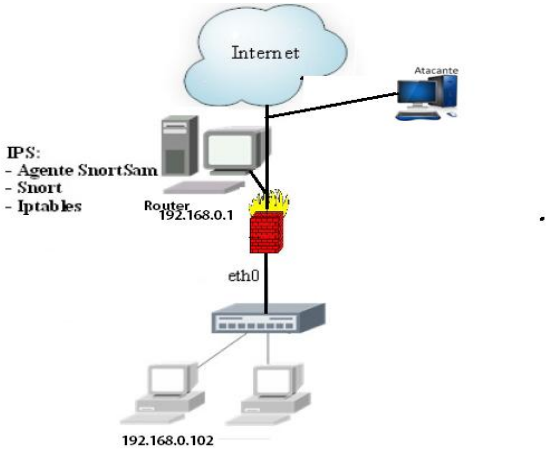


Ilustración 63.Muestra diseño de una red con una máquina debian que funciona como un Router e IPS.

Requisitos para el Diseño.

2 interfaz de red, Una para comunicarnos con el exterior y con la otra nos comunicaremos con el resto de computadoras. En nuestro caso se usará tarjetas de red Ethernet virtuales.

Se debe configurar las Iptables, para administrar conexiones y aplicar reglas, así mismo se deben configurar las reglas para el IDS .También se debe usar dnsmasq, para asignar ips y dns de forma automática a las máquinas.

Pasos.

Para este ejemplo hay conectado un servidor configurado con snort como IPS y que tiene una tarjeta libre, así mismo se observa un firewall que permite filtrar el tràfico de la red y denegar ciertas solicitudes no deseadas.

Serían Eth0 y Eth1 respectivamente.

Se debe acceder al archivo */etc/network/interfaces* y editar dicho archivo.

sudo nano /etc/network/interfaces

Para configurar el contenido se debe escribir lo siguiente:

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet dhcp

En este caso se ha logrado configurar la tarjeta de red eth0 para obtener ip por dhcp, pero no hay existen configuraciones para eth1, entonces se procede a configurar y crear una red con dicha interfaz. El archivo queda de la siguiente manera:

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet dhcp

auto eth1

iface eth1 inet static

address 192.168.0.1

netmask 255.255.255.0

broadcast 192.168.0.255

Por último se guarda la configuración realizada y se debe tener en cuenta que la configuraciòn quede de la siguiente manera.

Ip de la máquina es 192.168.0.1

La máscara de red es 255.255.255.0

Y la dirección de difusión es la 192.168.0.103

Para que sean efectivos los cambios se debe de reiniciar el servicio de red.

sudo /etc/init.d/netwoking restart

Luego se debe proceder activar ip_forward para que el servidor no ignore ciertos paquetes que no vayan destinados él, puesto que pueden ser paquetes para otros equipos y esto haría que esos equipos no tengan respuesta del exterior.

Para activarlo es posible realizarlo de dos formas:

1.Provisionalmente (Se pierde al reiniciar):

echo 1 > /proc/sys/net/ipv4/ip_forward

2.De manera permanente:

Editando el archivo */etc/sysctl.conf*

sudo nano /etc/sysctl.conf

Y quitar el comentario de la línea: #net.ipv4.ip_forward=1

Luego se procede a activar NAT para que los equipos que estén conectados al servidor debian puedan salir a internet mediante la ip del servidor que se logró configurar como router. En este caso nat realiza una bifurcación de los datos entre redes.

Para esto usaremos iptables con el siguiente comando:

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

A continuación se explica de manera breve: algunos comandos para entender su funcionamiento.

Iptables es el comando para modificar las reglas.

-t Es para especificar el tipo de tabla a la que van dirigidas las reglas.

nat Es el tipo de tabla.

-A Añade la regla a las que existen previamente.

POSTROUTING: Esta instrucción permite modificar los paquetes antes de reenviarlos a las máquinas correspondientes

-o Sirve para especificar hacía que tarjeta van redirigidos los paquetes.

eth0 Es nuestra tarjeta conectada a internet.

-j Específica hacia donde se aplican las reglas

MASQUERADE Indica el enmascaramiento ip.

En pocas palabras lo que se configuró fue, que todo lo que entre a nuestro servidor por la tarjeta que no sea eth0 se enmascara y se reenvía a la tarjeta eth0.

Consulta tomada de http://www.debianchile.org/router

Reglas de ips.

Las reglas del IPS que se deben configurar para que servidor rechace peticiones que puedan causar denegación de servicios distribuidos y DOS, al tiempo debemos configurarlo para que filtre el tráfico entrante y saliente de la red.

A continuación se define la configuración para el firewall.

```
ptables -N udp-flood
iptables -A OUTPUT -p udp -j udp-flood
iptables -A udp-flood -p udp -m limit --limit 50/s -j RETURN
iptables -A udp-flood -j LOG --log-level 4 --log-prefix 'UDP-flood
attempt: '
iptables -A udp-flood -j DROP
```

Ilustración 64.Configuración de Firewall

También es necesario definir reglas para evitar ser víctimas de sniffer, ICMP, DNS y ataques de amplificación de SNMP.

En la siguiente ilustración se muestra desde otro ordenador con dirección IP 192.168.0.103 se envía un ataque al IPS 192.168.0.1 cómo se puede ver en la ilustración , con idswakeup.

```
./idswakeup 192.168.0.103 192.168.0.1 100 64

  192.168.0.103 -> 192.168.0.1    23/tcp  ld_preload
  192.168.0.103 -> 192.168.0.1    23/tcp  ld_library_pat

sending : rlogin_bestof
          192.168.0.103 -> 192.168.0.1   513/tcp  IFS=/
          192.168.0.103 -> 192.168.0.1   513/tcp  su - root

sending : tcpflag_bestof ...
          192.168.0.103 -> 192.168.0.1   80/tcp -SF
          192.168.0.103 -> 192.168.0.1   80/tcp -SR
          192.168.0.103 -> 192.168.0.1   80/tcp
          192.168.0.103 -> 192.168.0.1   80/tcp -A
          192.168.0.103 -> 192.168.0.1   80/tcp -SFR
          192.168.0.103 -> 192.168.0.1   80/tcp -SFARPXY
          192.168.0.103 -> 192.168.0.1   80/tcp -SA
```

Ilustración 65.Ataque ./idswakeup 192.168.0.103 a 192.168.0.1 100 64

Cuando se envía el ataque se observa el bloqueo a la dirección IP 192.168.0.103 equipo dispuesto para atacar, y se bloquea esa dirección IP por 5 minutos, así mismo todas las peticiones se bloquean de la ip 192.168.0.103 a la ip destino 192.168.0.1.

El bloqueo a equipo atacante

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp any
ACCEPT     esp  --  anywhere             anywhere
ACCEPT     ah   --  anywhere             anywhere
ACCEPT     udp  --  anywhere             224.0.0.251         udp dpt:mdns
ACCEPT     udp  --  anywhere             anywhere            udp dpt:ipp
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ipp
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:s
sh
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:h
ttp
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:f
tp
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:h
ttps
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:s
mtp
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:d
omain
ACCEPT     udp  --  anywhere             anywhere            state NEW udp dpt:d
omain
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:m
ysql
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:8
99
REJECT     all  --  anywhere             anywhere            reject-with icmp-ho
st-prohibited
```

Ilustración 66.el bloqueo a la dirección IP 192.168.0.103

6.3.7.DLP

Para esta prueba se realizó la instalación de dos herramientas de DLP de distintas marcas, la instalación se hizo en una maquina virtual (servidor windows 2008R2), cada uno por separado. Para verificar su nivel de efectividad para prevenir la fuga de información por difrentes vectores y validar las solicitudes realizadas en la red hospitalaria desde cualquier punto para la extracción de información

Esto se logró mediante las políticas y agentes que se crearon en las herramientas, en donde se evidencia que permite bloquear la extracción de información haciendo uso medios tales como ftp y correos electrónicos dando un nivel de efectividad Excelente. También se logró identificar unos modelos para la prevenir la fuga de información, uno de los considerados en esta tesis es la que proponen las soluciones DLP, esta solución de divide en 4 vectores para la prevención: Vector de red.(Monitoreo de la información que viaja en la red), Vector de puntos finales, vector almacenamiento y vector en la nube, todos los anteriores permiten hacer monitoreo.

Estas pruebas se realiza la instalación y en puesta en marcha de la solución de Symantec DLP, MCAFEE Data Loss Prevention y la implementación del Servidor para asegurar el perímetro se realizará lo siguiente.

1. Instalación y Configuración del Servidor (Windows Server 2008 R2).
2. Instalación y Configuración de la herramienta EndForce.
3. Instalación y Configuración de la herramienta EndPoint.
4. Instalación y Configuración del Agente.
5. Pruebas de Funcionalidad del sistema.

A continuación se muestra el esquema de pruebas que se construyó.

Figura 43 Esquema de pruebas

A continuación se muestran los resultados de las pruebas DLP con medios extraibles, HTTPS.

Descripción de la prueba	La prueba se hizo con la finalidad de comprobar la captura de incidentes por parte de Endpoint prevent en medios extraíbles al copiar o guardar información confidencial en una organización.
Pasos a seguir	1. Se Crea una política de prueba que detecte una expresión regular de RFCS
	2. Crear y copiar un archivo a un dispositivo extraíble que contenga información confidencial de RFC
	3. Verificar que el archivo se trasmitió correctamente.
	4. verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint.
Herramienta	1. DLP detecta y reporta el incidente.
Resultados esperados	2. Se evidencio que todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección es inmediata del incidente en la consola.
Efectividad	Excelente
Fase del APT donde aplica	6

Tabla 71.Detección de Medios Extraibles
Fuente de elaboración propia

Pruebas de Detección en HTTPS

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes en el protocolo Web HTTPS.
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave o expresiones regulares.
	2. Escribir un mensaje que contenga información confidencial y enviarlo desde un correo electrónico WEB que utilice cifrado HTTPS.
	3. Verificar el correcto envió del correo electrónico.
	4. Verificar la correcta detención de los incidentes a través del reporte
	1. Herramienta DLP reporta el incidente
Resultados esperados	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
Herramienta	3. La detección del incidente se realiza con prontitud en la consola
Efectividad	Excelente
Fase del APT donde aplica	6

Tabla 72. Pruebas de HTTPS

Fuente de elaboración propia

Prueba contra fuga de información

Descripción de la prueba	La prueba tiene como objetivo comprobar la funcionalidad de bloqueo de fuga de información confidencial.
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras o expresiones regulares.
	2. Anadir una regla de bloqueo de fuga de información confidencial.
	3. Enviar un correo electrónico que en él cuerpo del mensaje escribir las palabras o expresiones configuradas en la política de prueba.
	4. Verificar que aparezca la ventana de bloqueo y que el archivo no se envió.
	6. Verificar la correcta detección de los incidentes a través del reporte
	1. DLP detecta y reporta el incidente
Resultados esperados	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza en la consola.
Efectividad	Excelente
Fase APT que aplica	2, 3, 5 y 6

Tabla 73. Prueba contra fuga de información

A continuacion en la ilustración se muestra algunas ilustraciones de configuración de la herramienta DLP.

Configuración de un servidor de detección Sistema

Ilustración 67.Configuración del servidor de detección

Configuración de Alertas del

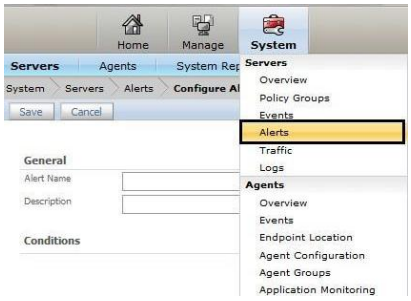


Ilustración 68. Alertas del sistema

Configuración del tráfico de la red

Configuración para la captura de logs

Ilustración 69. Configuración tráficodel sistema

Ilustración 70. configuración Captura de logs

Creamos políticas para nuestro servidor

Ilustración 71.Políticas DLP

Para este caso se selecciona la platilla HIPAA.

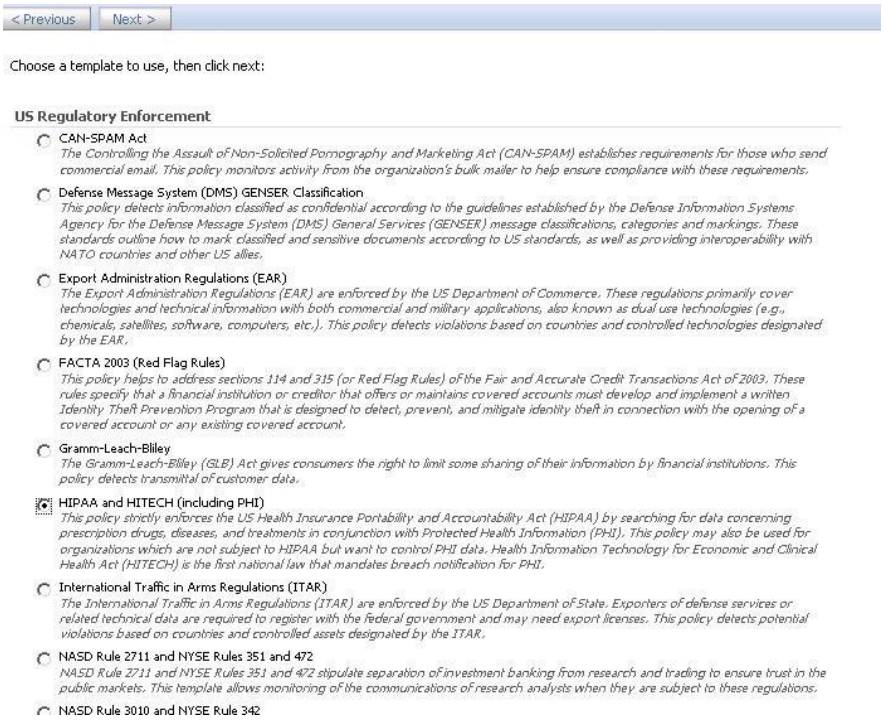


Ilustración 72: plantilla HIPAA

Resultados de DLP en medios extraibles.

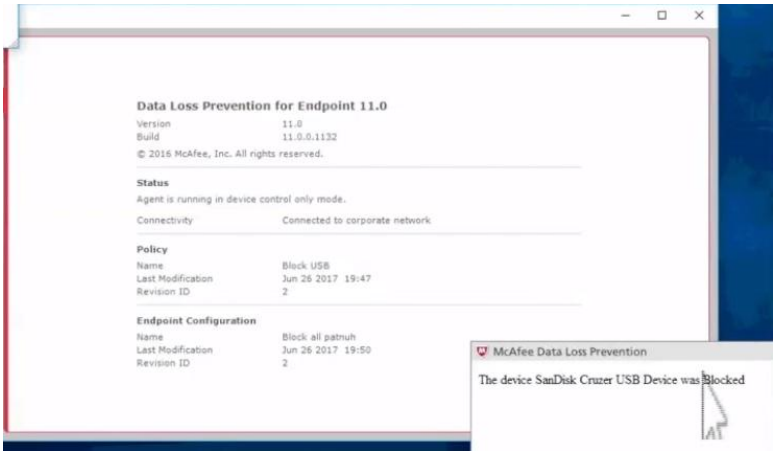


Ilustración 73. Bloqueo de medios extraibles

Resultados que se verían en caso de extraer información via correo.

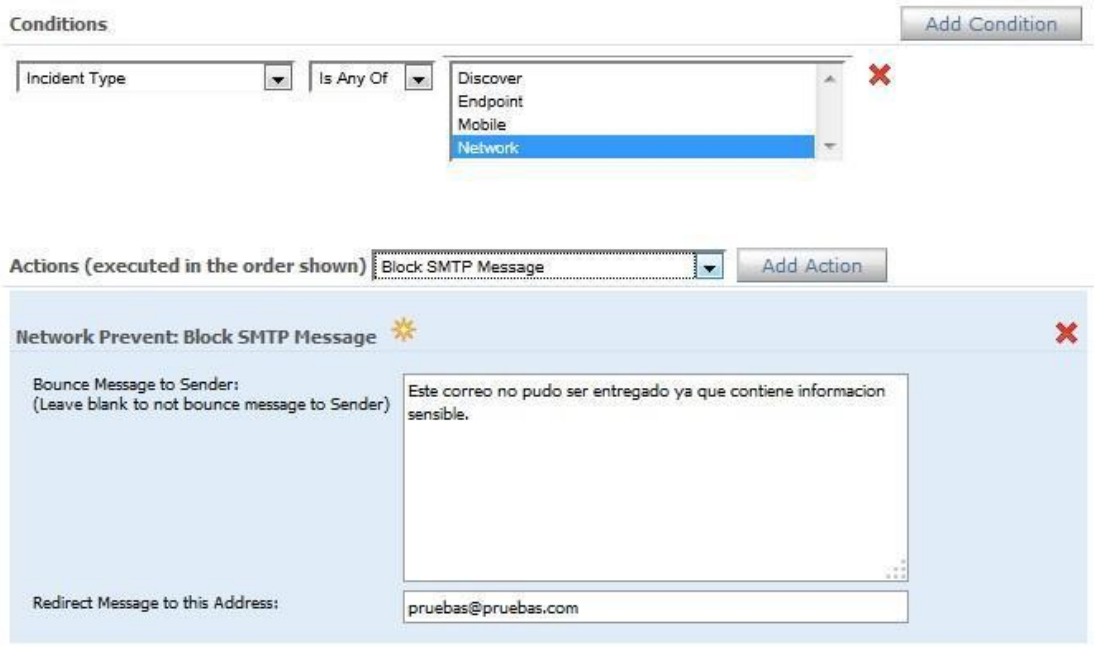


Ilustración 74. Bloqueo de fuga por correo

6.4. Anexo D. Pruebas del framework de seguridad informática.

A continuación se muestra el funcionamiento del framework de seguridad informática propuesto para las entidades hospitalarias en Colombia. Se siguieron los pasos descritos a continuación.

Registro Activos de acuerdo a la guía propuesta en el ítem 3.1, y como lo propone el artefacto del anexo A, ítem 6.1.(para este caso se realizo un software que recibe dichas entradas).

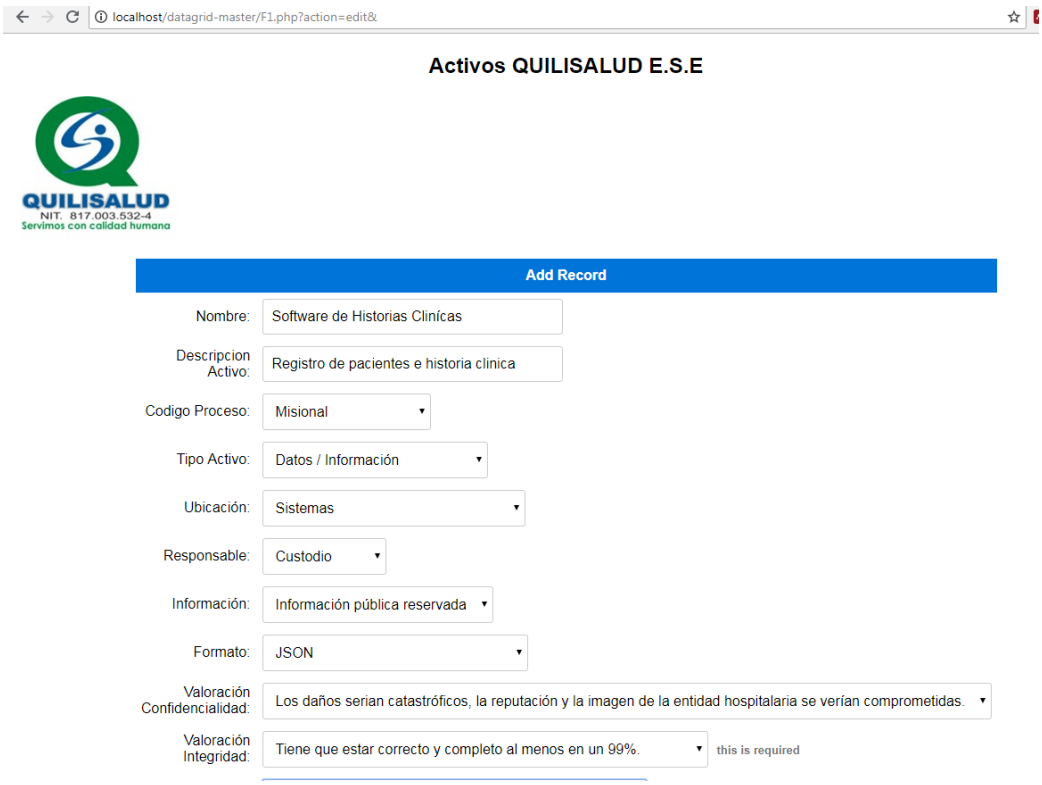
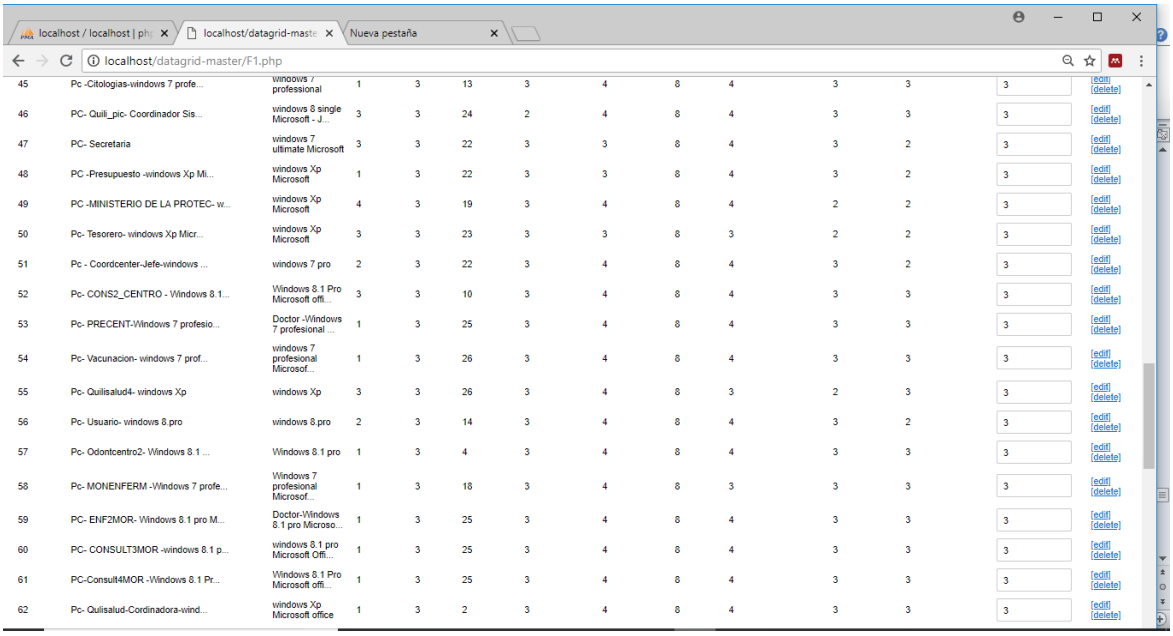


Ilustración 75. Registro de Activos

A continuación se clasifica los activos de la entidad hospitalaria objeto de estudio.

Lista de Activos registrados según artefacto propuesto en el anexo A, siguiendo los pasos de la guía propuesta en el ítem 3.1.

29	Equipo de rayos x ELITY 70 S/0...	NAP MONDOMO	3	6	4	1	3	8	3	2	2	3
30	Equipo de Escritorio SO. 8.1 ...	Intel pentium dual core E5700	1	3	4	3	3	8	4	3	3	3
31	Equipo de Escritorio SO. 8.1 ...	AMD Athlon 64 3000	1	3	4	3	3	8	4	2	3	3
32	Equipo Compaq 18 windows 8.1 P...	Intel Celeron j1800	1	3	4	3	4	8	4	3	3	3
33	Sony PAI_MONDOMO-PC windows 7...	Herramientas ofimáticas si	1	3	17	3	4	8	4	3	3	3
34	PC Sion Windows 7 ultimate	Tarjeta de RED si Herramienta ...	1	3	18	3	4	8	4	3	3	3
35	PC Sion MonCons3 Windows 8.1 ...	En red	1	3	19	3	3	8	3	3	3	3
36	PC FACTURACIÓNMOND Windows xp,...	Microsoft Office 2007 equipo e...	1	3	20	3	3	8	3	3	3	3
37	PC Compumax FACTURACION CENTRO...	En red, Instalado Java update	1	3	21	3	3	8	3	3	3	3
38	PC Lenovo- Windows 8.1 single ...	En RED si Software Instalado s...	1	3	22	3	4	8	4	3	3	3
39	Pc- SAMSUNG- Contabilidad- Win...	Windows 2007 Microsoft office ...	2	3	23	3	3	8	4	3	2	3
40	Pc-Contratacion -windows 7 ult...	windows 7 ultimate microsoft o...	3	3	22	3	2	8	3	2	2	2
41	Pc- Citologia- windows 8,1 pro...	windows 8,1 pro microsoft Offi...	1	3	13	3	4	8	4	3	3	3
42	Pc -sistemas2 -windows 10 micr...	windows 10 microsoft office 20...	3	3	24	2	4	8	4	3	3	3
43	PC -ARCHIVO CENTRO- windows xp...	windows xp 2002 microsoft offi...	1	3	22	3	4	8	4	3	3	3
44	PC- Factcentro- windows 7 ulti...	windows 7 ultimate	3	3	20	3	3	8	4	3	3	3
45	Pc -Citologias-windows 7 profe...	windows 7 professional	1	3	13	3	4	8	4	3	3	3



45	Pc -Citologias-windows 7 profe...	windows 7 professional	1	3	13	3	4	8	4	3	3	3
46	PC- Quil_pic- Coordinador Sis...	windows 8 single Microsoft - J...	3	3	24	2	4	8	4	3	3	3
47	PC- Secretaria	windows 7 ultimate Microsoft	3	3	22	3	3	8	4	3	2	3
48	PC -Presupuesto -windows Xp Mi...	windows Xp Microsoft	1	3	22	3	3	8	4	3	2	3
49	PC -MINISTERIO DE LA PROTEC- w...	windows Xp Microsoft	4	3	19	3	4	8	4	2	2	3
50	Pc- Tesorero- windows Xp Micr...	windows Xp Microsoft	3	3	23	3	3	8	3	2	2	3
51	Pc - Coordcenter-Jefe-windows ...	windows 7 pro	2	3	22	3	4	8	4	3	2	3
52	Pc- CONS2_CENTRO - Windows 8.1...	Windows 8.1 Pro Microsoft offi...	3	3	10	3	4	8	4	3	3	3
53	Pc- PRECENT-Windows 7 profesio...	Doctor -Windows 7 profesional ...	1	3	25	3	4	8	4	3	3	3
54	Pc- Vacunacion- windows 7 prof...	windows 7 profesional Microsof...	1	3	26	3	4	8	4	3	3	3
55	Pc- Quilisalud4- windows Xp	windows Xp	3	3	26	3	4	8	3	2	3	3
56	Pc- Usuario- windows 8.pro	windows 8.pro	2	3	14	3	4	8	4	3	2	3
57	Pc- Odontcentro2- Windows 8.1 ...	Windows 8.1 pro	1	3	4	3	4	8	4	3	3	3
58	Pc- MONENFERM -Windows 7 profe...	Windows 7 profesional Microsof...	1	3	18	3	4	8	3	3	3	3
59	PC- ENF2MOR- Windows 8.1 pro M...	Doctor-Windows 8.1 pro Microso...	1	3	25	3	4	8	4	3	3	3
60	PC- CONSULT3MOR -windows 8.1 p...	windows 8.1 pro Microsoft Offi...	1	3	25	3	4	8	4	3	3	3
61	PC-Consult4MOR -Windows 8.1 Pr...	Windows 8.1 Pro Microsoft offi...	1	3	25	3	4	8	4	3	3	3
62	Pc- Qulisalud-Cordinadora-wind...	windows Xp Microsoft office	1	3	2	3	4	8	4	3	3	3

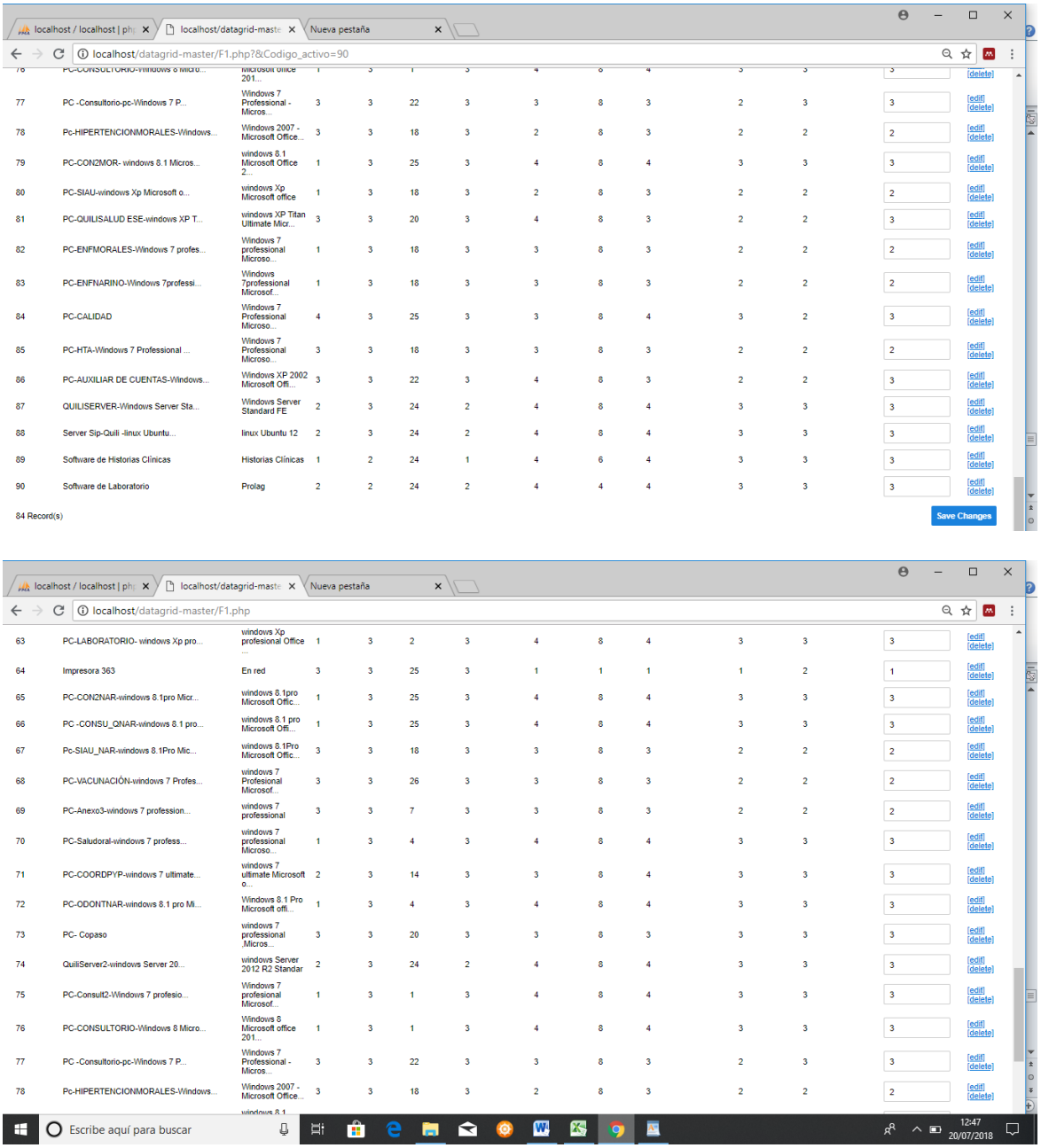


Ilustración 76.Lista de Activos registrados

Activos con Amenazas en orden de la leyenda

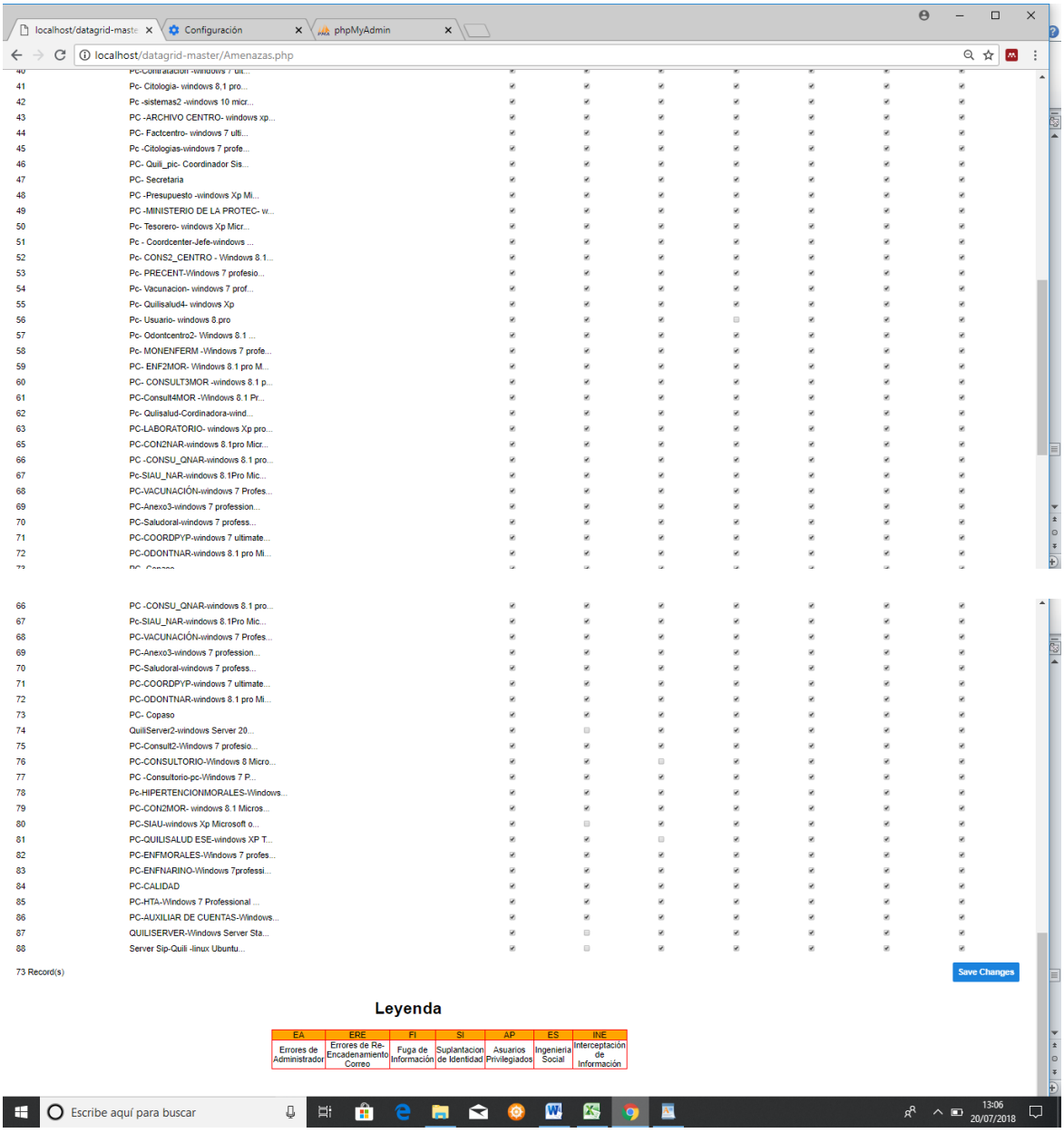


Ilustración 77. Activos vs Amenazas

Calculando nivel de fuga

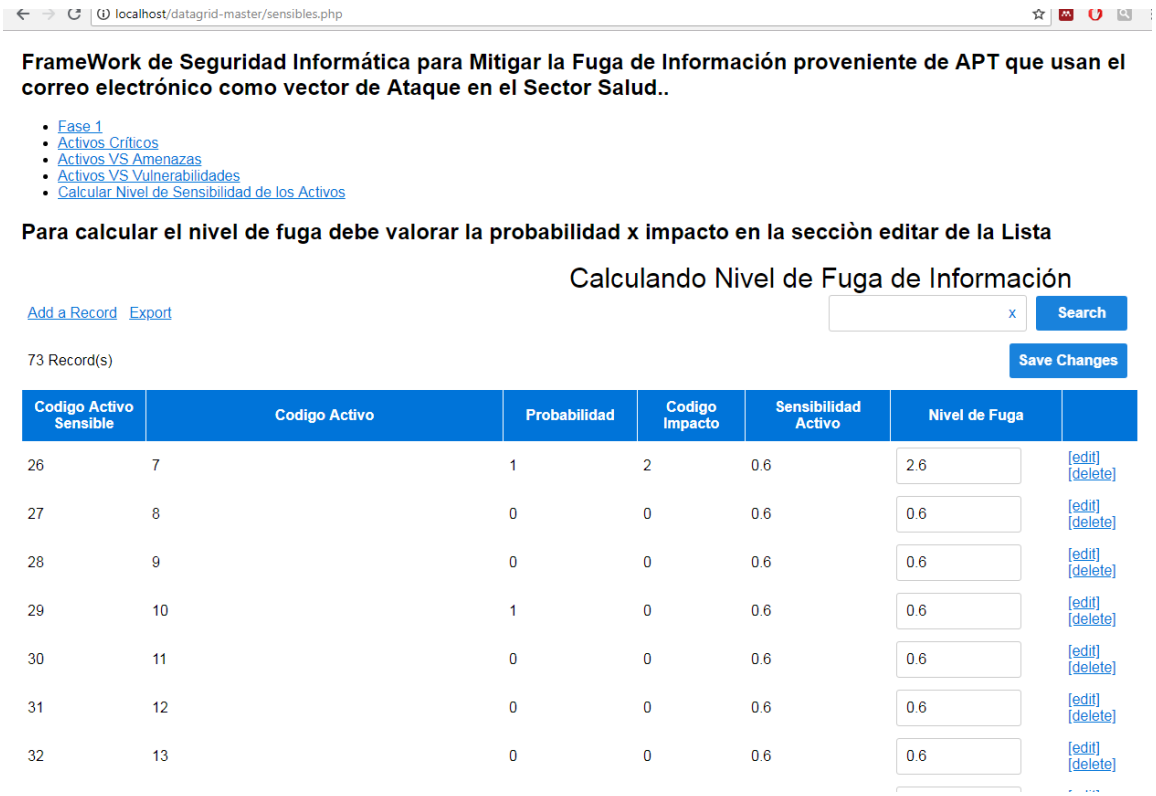
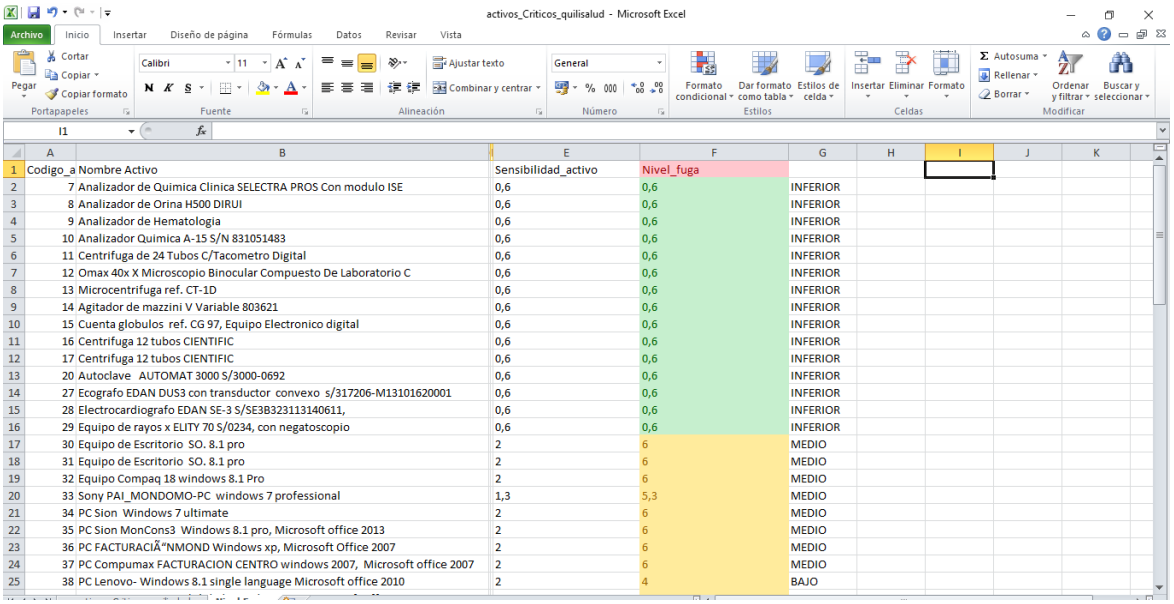


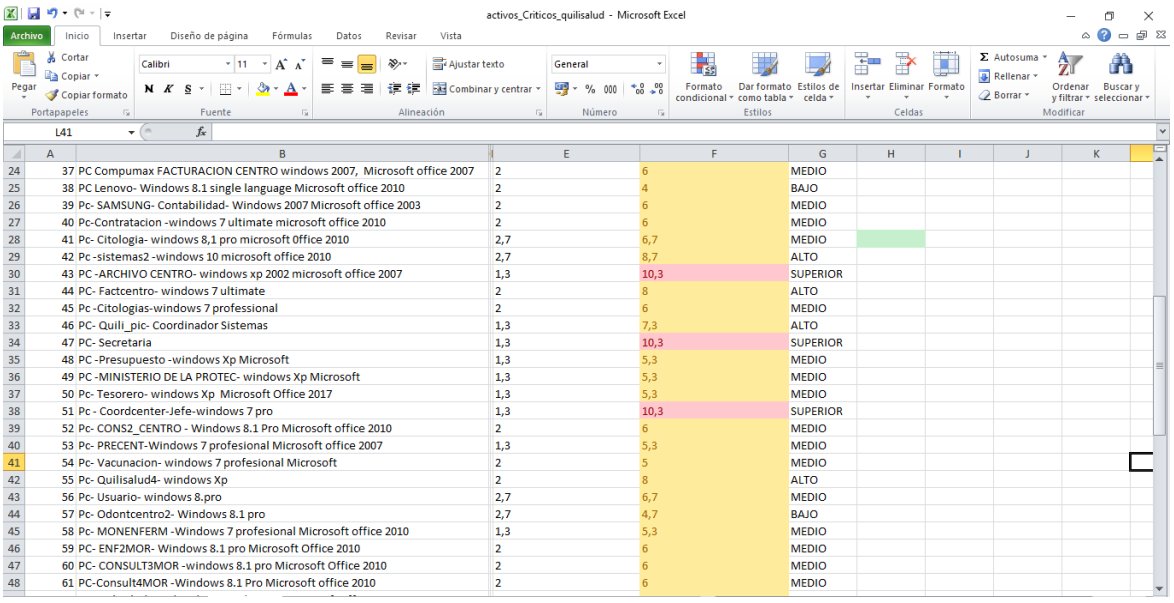
Ilustración 78. Nivel de fuga

Archivo Excel con activos con su respectivo nivel de fuga.



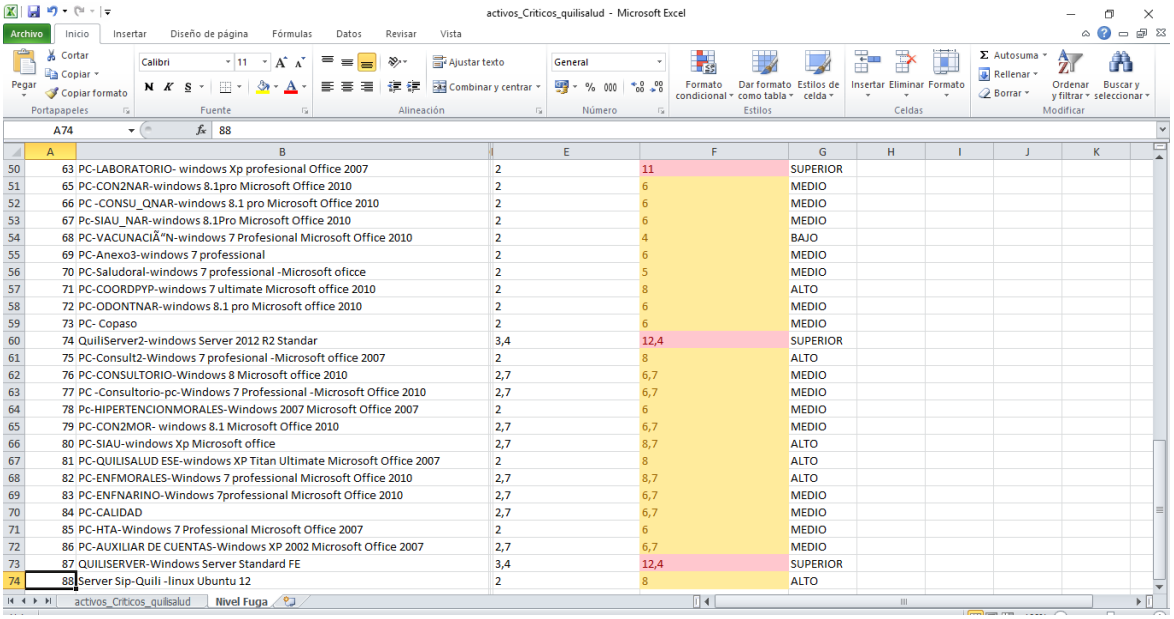
activos_Criticos_quilisalud - Microsoft Excel

Codigo_a	Nombre Activo	Sensibilidad_activo	Nivel_fuga	
7	Analizador de Quimica Clinica SELECTRA PROS Con modulo ISE	0,6	0,6	INFERIOR
8	Analizador de Orina H500 DIRUI	0,6	0,6	INFERIOR
9	Analizador de Hematologia	0,6	0,6	INFERIOR
10	Analizador Quimica A-15 S/N 831051483	0,6	0,6	INFERIOR
11	Centrifuga de 24 Tubos C/Tacometro Digital	0,6	0,6	INFERIOR
12	Omax 40x X Microscopio Binocular Compuesto De Laboratorio C	0,6	0,6	INFERIOR
13	Microcentrifuga ref. CT-1D	0,6	0,6	INFERIOR
14	Agitador de mazzini V Variable 803621	0,6	0,6	INFERIOR
15	Cuenta globulos ref. CG 97, Equipo Electronico digital	0,6	0,6	INFERIOR
16	Centrifuga 12 tubos CIENTIFIC	0,6	0,6	INFERIOR
17	Centrifuga 12 tubos CIENTIFIC	0,6	0,6	INFERIOR
20	Autoclave AUTOMAT 3000 S/3000-0692	0,6	0,6	INFERIOR
27	Ecografo EDAN DUS3 con transductor convexo s/317206-M13101620001	0,6	0,6	INFERIOR
28	Electrocardiografo EDAN SE-3 S/SE3B323113140611,	0,6	0,6	INFERIOR
29	Equipo de rayos x ELITY 70 S/0234, con negatoscopio	0,6	0,6	INFERIOR
30	Equipo de Escritorio SO. 8.1 pro	2	6	MEDIO
31	Equipo de Escritorio SO. 8.1 pro	2	6	MEDIO
32	Equipo Compaq 18 windows 8.1 Pro	2	6	MEDIO
33	Sony PAI_MONDOMO-PC windows 7 professional	1,3	5,3	MEDIO
34	PC Sion Windows 7 ultimate	2	6	MEDIO
35	PC Sion MonCons3 Windows 8.1 pro, Microsoft office 2013	2	6	MEDIO
36	PC FACTURACIÃ"NMOND Windows xp, Microsoft Office 2007	2	6	MEDIO
37	PC Compumax FACTURACION CENTRO windows 2007, Microsoft office 2007	2	6	MEDIO
38	PC Lenovo- Windows 8.1 single language Microsoft office 2010	2	4	BAJO



activos_Criticos_quilisalud - Microsoft Excel

37	PC Compumax FACTURACION CENTRO windows 2007, Microsoft office 2007	2	6	MEDIO
38	PC Lenovo- Windows 8.1 single language Microsoft office 2010	2	4	BAJO
39	Pc- SAMSUNG- Contabilidad- Windows 2007 Microsoft office 2003	2	6	MEDIO
40	Pc-Contratacion -windows 7 ultimate microsoft office 2010	2	6	MEDIO
41	Pc- Citologia- windows 8,1 pro microsoft 0ffice 2010	2,7	6,7	MEDIO
42	Pc -sistemas2 -windows 10 microsoft office 2010	2,7	8,7	ALTO
43	PC -ARCHIVO CENTRO- windows xp 2002 microsoft office 2007	1,3	10,3	SUPERIOR
44	PC- Factcentro- windows 7 ultimate	2	8	ALTO
45	Pc -Citologias-windows 7 professional	2	6	MEDIO
46	PC- Quili_pic- Coordinador Sistemas	1,3	7,3	ALTO
47	PC- Secretaria	1,3	10,3	SUPERIOR
48	PC -Presupuesto -windows Xp Microsoft	1,3	5,3	MEDIO
49	PC -MINISTERIO DE LA PROTEC- windows Xp Microsoft	1,3	5,3	MEDIO
50	Pc- Tesorero- windows Xp Microsoft Office 2017	1,3	5,3	MEDIO
51	Pc - Coordcenter-Jefe-windows 7 pro	1,3	10,3	SUPERIOR
52	Pc- CONS2_CENTRO - Windows 8.1 Pro Microsoft office 2010	2	6	MEDIO
53	Pc- PRECENT-Windows 7 profesional Microsoft office 2007	1,3	5,3	MEDIO
54	Pc- Vacunacion- windows 7 profesional Microsoft	2	5	MEDIO
55	Pc- Quilisalud4- windows Xp	2	8	ALTO
56	Pc- Usuario- windows 8.pro	2,7	6,7	MEDIO
57	Pc- Odontcentro2- Windows 8.1 pro	2,7	4,7	BAJO
58	Pc- MONENFERM -Windows 7 profesional Microsoft office 2010	1,3	5,3	MEDIO
59	PC- ENF2MOR- Windows 8.1 pro Microsoft Office 2010	2	6	MEDIO
60	PC- CONSULT3MOR -windows 8.1 pro Microsoft Office 2010	2	6	MEDIO
61	PC-Consult4MOR -Windows 8.1 Pro Microsoft office 2010	2	6	MEDIO



	A	B	E	F	G
50	63	PC-LABORATORIO- windows Xp profesional Office 2007	2	11	SUPERIOR
51	65	PC-CON2NAR-windows 8.1pro Microsoft Office 2010	2	6	MEDIO
52	66	PC -CONSU_QNAR-windows 8.1 pro Microsoft Office 2010	2	6	MEDIO
53	67	Pc-SIAU_NAR-windows 8.1Pro Microsoft Office 2010	2	6	MEDIO
54	68	PC-VACUNACIÃ"N-windows 7 Profesional Microsoft Office 2010	2	4	BAJO
55	69	PC-Anexo3-windows 7 professional	2	6	MEDIO
56	70	PC-Saludoral-windows 7 professional -Microsoft oficce	2	5	MEDIO
57	71	PC-COORDPYP-windows 7 ultimate Microsoft office 2010	2	8	ALTO
58	72	PC-ODONTNAR-windows 8.1 pro Microsoft office 2010	2	6	MEDIO
59	73	PC- Copaso	2	6	MEDIO
60	74	QuiliServer2-windows Server 2012 R2 Standar	3,4	12,4	SUPERIOR
61	75	PC-Consult2-Windows 7 profesional -Microsoft office 2007	2	8	ALTO
62	76	PC-CONSULTORIO-Windows 8 Microsoft office 2010	2,7	6,7	MEDIO
63	77	PC -Consultorio-pc-Windows 7 Professional -Microsoft Office 2010	2,7	6,7	MEDIO
64	78	Pc-HIPERTENCIONMORALES-Windows 2007 Microsoft Office 2007	2	6	MEDIO
65	79	PC-CON2MOR- windows 8.1 Microsoft Office 2010	2,7	6,7	MEDIO
66	80	PC-SIAU-windows Xp Microsoft office	2,7	8,7	ALTO
67	81	PC-QUILISALUD ESE-windows XP Titan Ultimate Microsoft Office 2007	2	8	ALTO
68	82	PC-ENFMORALES-Windows 7 professional Microsoft Office 2010	2,7	8,7	ALTO
69	83	PC-ENFNARINO-Windows 7professional Microsoft Office 2010	2,7	6,7	MEDIO
70	84	PC-CALIDAD	2,7	6,7	MEDIO
71	85	PC-HTA-Windows 7 Professional Microsoft Office 2007	2	6	MEDIO
72	86	PC-AUXILIAR DE CUENTAS-Windows XP 2002 Microsoft Office 2007	2,7	6,7	MEDIO
73	87	QUILISERVER-Windows Server Standard FE	3,4	12,4	SUPERIOR
74	88	Server Sip-Quili -linux Ubuntu 12	2	8	ALTO

Ilustración 79. Activos con nivel de fuga

Activos con nivel de fuga Media, Alto y superior

40	53	Pc- PRECENT-Windows 7 profesional Microsoft office 2007	2	1,3	5,3	MEDIO
41	54	Pc- Vacunacion- windows 7 profesional Microsoft	1	2	5	MEDIO
42	55	Pc- Quilisalud4- windows Xp	2	2	8	ALTO
43	56	Pc- Usuario- windows 8.pro	2	2,7	6,7	MEDIO
45	58	Pc- MONENFERM -Windows 7 profesional Microsoft office 2010	2	1,3	5,3	MEDIO
46	59	PC- ENF2MOR- Windows 8.1 pro Microsoft Office 2010	2	2	6	MEDIO
47	60	PC- CONSULT3MOR -windows 8.1 pro Microsoft Office 2010	2	2	6	MEDIO
48	61	PC-Consult4MOR -Windows 8.1 Pro Microsoft office 2010	2	2	6	MEDIO
49	62	Pc- Qulisalud-Cordinadora-windows Xp Microsoft office	2	2	8	ALTO
50	63	PC-LABORATORIO- windows Xp profesional Office 2007	3	2	11	SUPERIOR
51	65	PC-CON2NAR-windows 8.1pro Microsoft Office 2010	2	2	6	MEDIO
52	66	PC -CONSU_QNAR-windows 8.1 pro Microsoft Office 2010	2	2	6	MEDIO
53	67	Pc-SIAU_NAR-windows 8.1Pro Microsoft Office 2010	2	2	6	MEDIO
55	69	PC-Anexo3-windows 7 professional	2	2	6	MEDIO
56	70	PC-Saludoral-windows 7 professional -Microsoft oficce	1	2	5	MEDIO
57	71	PC-COORDPYP-windows 7 ultimate Microsoft office 2010	2	2	8	ALTO
58	72	PC-ODONTNAR-windows 8.1 pro Microsoft office 2010	2	2	6	MEDIO
59	73	PC- Copaso	2	2	6	MEDIO
60	74	QuiliServer2-windows Server 2012 R2 Standar	3	3,4	12,4	SUPERIOR
61	75	PC-Consult2-Windows 7 profesional -Microsoft office 2007	2	2	8	ALTO
62	76	PC-CONSULTORIO-Windows 8 Microsoft office 2010	2	2,7	6,7	MEDIO
63	77	PC -Consultorio-pc-Windows 7 Professional -Microsoft Office 2010	2	2,7	6,7	MEDIO
64	78	Pc-HIPERTENCIONMORALES-Windows 2007 Microsoft Office 2007	2	2	6	MEDIO
65	79	PC-CON2MOR- windows 8.1 Microsoft Office 2010	2	2,7	6,7	MEDIO
66	80	PC-SIAU-windows Xp Microsoft office	2	2,7	8,7	ALTO
67	81	PC-QUILISALUD ESE-windows XP Titan Ultimate Microsoft Office 2007	2	2	8	ALTO
68	82	PC-ENFMORALES-Windows 7 professional Microsoft Office 2010	2	2,7	8,7	ALTO
69	83	PC-ENFNARINO-Windows 7professional Microsoft Office 2010	2	2,7	6,7	MEDIO
70	84	PC-CALIDAD	2	2,7	6,7	MEDIO
71	85	PC-HTA-Windows 7 Professional Microsoft Office 2007	2	2	6	MEDIO
72	86	PC-AUXILIAR DE CUENTAS-Windows XP 2002 Microsoft Office 2007	2	2,7	6,7	MEDIO
73	87	QUILISERVER-Windows Server Standard FE	3	3,4	12,4	SUPERIOR
74	88	Server Sip-Quili -linux Ubuntu 12	3	2	8	ALTO
75	90	Software de Laboratorio Clinico	3	3,4	12,4	SUPERIOR
76	89	Software de Historias Clinicas	3	3,4	12,4	SUPERIOR

Ilustración 80.Nivel de fuga superior, Medio y Alto

Activos con nivel de fuga comprometidos con sus respectivas amenazas

Codigo_A_A	Nombre_activo	AMENAZAS						
7	Analizador de Quimica Clinica SELECTRA PROS Con modulo ISE	EA						INE
8	Analizador de Orina H500 DIRUI	EA						INE
9	Analizador de Hematologia	EA						INE
10	Analizador Quimica A-15 S/N 831051483	EA						INE
11	Centrifuga de 24 Tubos C/Tacometro Digital	EA						
12	Omax 40x X Microscopio Binocular Compuesto De Laboratorio C	EA						
13	Microcentrifuga ref. CT-1D	EA						
14	Agitador de mazzini V Variable 803621	EA						
15	Cuenta globulos ref. CG 97, Equipo Electronico digital	EA						
16	Centrifuga 12 tubos CIENTIFIC	EA						
17	Centrifuga 12 tubos CIENTIFIC	EA						
20	Autoclave AUTOMAT 3000 S/3000-0692	EA						
27	Ecografo EDAN DUS3 con transductor convexo s/317206-M13101620001	EA						
28	Electrocardiografo EDAN SE-3 S/SE3B323113140611,	EA						
29	Equipo de rayos x ELITY 70 S/0234, con negatoscopio	EA						INE

30	Equipo de Escritorio SO. 8.1 pro	EA	ERE	FI	SI	AP	ES	INE
31	Equipo de Escritorio SO. 8.1 pro	EA	ERE	FI	SI	AP	ES	INE
32	Equipo Compaq 18 windows 8.1 Pro	EA	ERE	FI	SI	AP	ES	INE
33	Sony PAI_MONDOMO-PC windows 7 professional	EA	ERE	FI	SI	AP	ES	INE
34	PC Sion Windows 7 ultimate	EA	ERE	FI	SI	AP	ES	INE
35	PC Sion MonCons3 Windows 8.1 pro, Microsoft office 2013	EA	ERE	FI	SI	AP	ES	INE
36	PC FACTURACIÃ“NMOND Windows xp, Microsoft Office 2007	EA	ERE	FI	SI	AP	ES	INE
37	PC Compumax FACTURACION CENTRO windows 2007, Microsoft office 2007	EA	ERE	FI	SI	AP	ES	INE
38	PC Lenovo- Windows 8.1 single language Microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE
39	Pc- SAMSUNG- Contabilidad- Windows 2007 Microsoft office 2003	EA	ERE	FI	SI	AP	ES	INE
40	Pc-Contratacion -windows 7 ultimate microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE
41	Pc- Citologia- windows 8,1 pro microsoft 0ffice 2010	EA	ERE	FI	SI	AP	ES	INE
42	Pc -sistemas2 -windows 10 microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE
43	PC -ARCHIVO CENTRO- windows xp 2002 microsoft office 2007	EA	ERE	FI	SI	AP	ES	INE
44	PC- Factcentro- windows 7 ultimate	EA	ERE	FI	SI	AP	ES	INE
45	Pc -Citologias-windows 7 professional	EA	ERE	FI	SI	AP	ES	INE
46	PC- Quili_pic- Coordinador Sistemas	EA	ERE	FI	SI	AP	ES	INE
47	PC- Secretaria	EA	ERE	FI	SI	AP	ES	INE
48	PC -Presupuesto -windows Xp Microsoft	EA	ERE	FI	SI	AP	ES	INE
49	PC -MINISTERIO DE LA PROTEC- windows Xp Microsoft	EA	ERE	FI	SI	AP	ES	INE
50	Pc- Tesorero- windows Xp Microsoft Office 2017	EA	ERE	FI	SI	AP	ES	INE
51	Pc - Coordcenter-Jefe-windows 7 pro	EA	ERE	FI	SI	AP	ES	INE
52	Pc- CONS2_CENTRO - Windows 8.1 Pro Microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE
53	Pc- PRECENT-Windows 7 profesional Microsoft office 2007	EA	ERE	FI	SI	AP	ES	INE
54	Pc- Vacunacion- windows 7 profesional Microsoft	EA	ERE	FI	SI	AP	ES	INE
55	Pc- Quilisalud4- windows Xp	EA	ERE	FI	SI	AP	ES	INE
56	Pc- Usuario- windows 8.pro	EA	ERE	FI		AP	ES	INE
57	Pc- Odontcentro2- Windows 8.1 pro	EA	ERE	FI	SI	AP	ES	INE
58	Pc- MONENFERM -Windows 7 profesional Microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE
59	PC- ENF2MOR- Windows 8.1 pro Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
60	PC- CONSULT3MOR -windows 8.1 pro Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
61	PC-Consult4MOR -Windows 8.1 Pro Microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE

62	Pc- Qulisalud-Cordinadora-windows Xp Microsoft office	EA	ERE	FI	SI	AP	ES	INE
63	PC-LABORATORIO- windows Xp profesional Office 2007	EA	ERE	FI	SI	AP	ES	INE
65	PC-CON2NAR-windows 8.1pro Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
66	PC -CONSU_QNAR-windows 8.1 pro Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
67	Pc-SIAU_NAR-windows 8.1Pro Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
68	PC-VACUNACIÃ“N-windows 7 Profesional Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
69	PC-Anexo3-windows 7 professional	EA	ERE	FI	SI	AP	ES	INE
70	PC-Saludoral-windows 7 professional - Microsoft oficce	EA	ERE	FI	SI	AP	ES	INE
71	PC-COORDPYP-windows 7 ultimate Microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE
72	PC-ODONTNAR-windows 8.1 pro Microsoft office 2010	EA	ERE	FI	SI	AP	ES	INE
73	PC- Copaso	EA	ERE	FI	SI	AP	ES	INE
74	QuiliServer2-windows Server 2012 R2 Standar	EA		FI	SI	AP	ES	INE
75	PC-Consult2-Windows 7 profesional - Microsoft office 2007	EA	ERE	FI	SI	AP	ES	INE
76	PC-CONSULTORIO-Windows 8 Microsoft office 2010	EA	ERE		SI	AP	ES	INE
77	PC -Consultorio-pc-Windows 7 Professional -Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
78	Pc-HIPERTENCIONMORALES-Windows 2007 Microsoft Office 2007	EA	ERE	FI	SI	AP	ES	INE
79	PC-CON2MOR- windows 8.1 Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
80	PC-SIAU-windows Xp Microsoft office	EA		FI	SI	AP	ES	INE
81	PC-QUILISALUD ESE-windows XP Titan Ultimate Microsoft Office 2007	EA	ERE		SI	AP	ES	INE
82	PC-ENFMORALES-Windows 7 professional Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
83	PC-ENFNARINO-Windows 7professional Microsoft Office 2010	EA	ERE	FI	SI	AP	ES	INE
84	PC-CALIDAD	EA	ERE	FI	SI	AP	ES	INE
85	PC-HTA-Windows 7 Professional Microsoft Office 2007	EA	ERE	FI	SI	AP	ES	INE
86	PC-AUXILIAR DE CUENTAS-Windows XP 2002 Microsoft Office 2007	EA	ERE	FI	SI	AP	ES	INE
87	QUILISERVER-Windows Server Standard FE	EA		FI	SI	AP	ES	INE
88	Server Sip-Quili -linux Ubuntu 12	EA		FI	SI	AP	ES	INE

Leyendas			
[EA]	Errores de Administrador	[SI]	Suplantacion de identidad
[ERE]	Errores de Reencademamiento	[AP]	Usuarios Privelegiados
[FI]	Fuga de Informacion	[INE]	Interceptacion de información
		[ES]	Ingenieria Social

Ilustración 81.Activos Vs Amenazas

A continuación se muestra la salida que arroja el framework propuesto para el sector salud, el cuál es muy fácil de replicar, haciendo uso de los artefactos propuestos y aspectos metodológicos. Al final se lográ identificar un conjunto de activos sensibles a fuga de información(Ver ilustración 80) de una listado que fue tomado como referencia de una entidad hospitalaria (Ver ilustracion 76). A los cuales se les debe aplicar buenas prácticas y recomendaciones sobre uso de herramientas, teniendo en cuenta el riesgo que el framework identifico en la fase de ciclo de vida del APT. Para ello se deben remitir a contrastar el riesgo que esta asociado al activo en la ilustración 82, con las buenas prácticas propuestas (Ver ítem 3.2) y herramientas recomendadas para dicho riesgo (ver item 3.3).

En la siguiente tabla 82 se observan un listado de activos que se identificaron con posible nivel de fuga de información y con sus respectivos riesgos.

Nombre Activo	Codigo_probabilidad	Codigo_Impacto	Sensibilidad_activo	Nivel_fuga	Calificación	EA	ERE	FI	SI	AP	ES	INE
Equipo de Escritorio SO. 8.1 pro		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
Equipo de Escritorio SO. 8.1 pro		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de	Ingeniería social-Phishing	Pérdida de integridad de datos

										maquinas infectadas-Establecer conexión externas		
Equipo Compaq 18 windows 8.1 Pro		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

Sony PAI_MONDOMO-PC windows 7 professional		2	1,3	5,3	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC Sion Windows 7 ultimate		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC Sion MonCons3 Windows 8.1 pro, Microsoft office 2013		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC FACTURACIÃ“NMOND Windows xp, Microsoft Office 2007		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC Compumax FACTURACION CENTRO windows 2007, Microsoft office 2007		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
Pc- SAMSUNG-Contabilidad- Windows 2007 Microsoft office 2003		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

Pc-Contratacion - windows 7 ultimate microsoft office 2010		2	2	6	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control remoto de maquinas infectadas- Establecer conexión externas	Ingeniería social- Phishing	Pérdida de integridad de datos
Pc- Citologia- windows 8,1 pro microsoft 0ffice 2010		2	2,7	6,7	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control	Ingeniería social- Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
Pc -sistemas2 -windows 10 microsoft office 2010		2	2,7	8,7	ALTO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC -ARCHIVO CENTRO- windows xp 2002 microsoft office 2007		3	1,3	10,3	SUPERIOR	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC- Factcentro-windows 7 ultimate		3	2	8	ALTO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
Pc -Citologias-windows 7 professional		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC- Quili_pic-Coordinador Sistemas		3	1,3	7,3	ALTO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC- Secretaria		3	1,3	10,3	SUPERIOR	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC -Presupuesto - windows Xp Microsoft		2	1,3	5,3	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC -MINISTERIO DE LA PROTEC- windows Xp Microsoft		2	1,3	5,3	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control remoto de maquinas infectadas- Establecer conexión externas	Ingeniería social- Phishing	Pérdida de integridad de datos
Pc- Tesorero- windows Xp Microsoft Office 2017		2	1,3	5,3	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control	Ingeniería social- Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
Pc - Coordcenter-Jefe-windows 7 pro		3	1,3	10,3	SUPERIOR	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

Pc- CONS2_CENTRO - Windows 8.1 Pro Microsoft office 2010		2	2	6	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control remoto de maquinas infectadas- Establecer conexión externas	Ingeniería social- Phishing	Pérdida de integridad de datos
Pc- PRECENT- Windows 7 profesional Microsoft office 2007		2	1,3	5,3	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control	Ingeniería social- Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
Pc- Vacunacion-windows 7 profesional Microsoft		1	2	5	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

Pc- Quilisalud4- windows Xp		2	2	8	ALTO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control remoto de maquinas infectadas- Establecer conexión externas	Ingeniería social- Phishing	Pérdida de integridad de datos
Pc- Usuario- windows 8.pro		2	2,7	6,7	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	#N/A	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control	Ingeniería social- Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
Pc- MONENFERM - Windows 7 profesional Microsoft office 2010		2	1,3	5,3	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC- ENF2MOR- Windows 8.1 pro Microsoft Office 2010		2	2	6	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control remoto de maquinas infectadas- Establecer conexión externas	Ingeniería social- Phishing	Pérdida de integridad de datos
PC- CONSULT3MOR - windows 8.1 pro Microsoft Office 2010		2	2	6	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control	Ingeniería social- Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC-Consult4MOR - Windows 8.1 Pro Microsoft office 2010		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

Pc- Qulisalud-Cordinadora-windows Xp Microsoft office		2	2	8	ALTO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC-LABORATORIO-windows Xp profesional Office 2007		3	2	11	SUPERIOR	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC-CON2NAR-windows 8.1pro Microsoft Office 2010		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC -CONSU_QNAR-windows 8.1 pro Microsoft Office 2010		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
Pc-SIAU_NAR-windows 8.1Pro Microsoft Office 2010		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC-Anexo3-windows 7 professional		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC-Saludoral-windows 7 professional - Microsoft office		1	2	5	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control remoto de maquinas infectadas- Establecer conexión externas	Ingeniería social- Phishing	Pérdida de integridad de datos
PC-COORDPYP- windows 7 ultimate Microsoft office 2010		2	2	8	ALTO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control	Ingeniería social- Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC-ODONTNAR-windows 8.1 pro Microsoft office 2010		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC- Copaso		2	2	6	MEDIO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero- Explotación de equipos- Ingeniería social- Phishing- Sitios maliciosos- Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control remoto de maquinas infectadas- Establecer conexión externas	Ingeniería social- Phishing	Pérdida de integridad de datos
QuiliServer2-windows Server 2012 R2 Standar		3	3,4	12,4	SUPERIOR	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	#N/A	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control	Ingeniería social- Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC-Consult2-Windows 7 profesional -Microsoft office 2007		2	2	8	ALTO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC-CONSULTORIO-Windows 8 Microsoft office 2010		2	2,7	6,7	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	#N/A	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC -Consultorio-pc-Windows 7 Professional -Microsoft Office 2010		2	2,7	6,7	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
Pc-HIPERTENCIONMORALES-Windows 2007 Microsoft Office 2007		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC-CON2MOR-windows 8.1 Microsoft Office 2010		2	2,7	6,7	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC-SIAU-windows Xp Microsoft office		2	2,7	8,7	ALTO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	0	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC-QUILISALUD ESE-windows XP Titan Ultimate Microsoft Office 2007		2	2	8	ALTO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	0	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC-ENFMORALES-Windows 7 professional Microsoft Office 2010		2	2,7	8,7	ALTO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC-ENFNARINO-Windows 7professional Microsoft Office 2010		2	2,7	6,7	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
PC-CALIDAD		2	2,7	6,7	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

PC-HTA-Windows 7 Professional Microsoft Office 2007		2	2	6	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos
PC-AUXILIAR DE CUENTAS-Windows XP 2002 Microsoft Office 2007		2	2,7	6,7	MEDIO	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	Vulnerabilidades del dia cero-Explotación de equipos-Ingeniería social-Phishing-Sitios maliciosos-Robo de información	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control	Ingeniería social-Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
QUILISERVER-Windows Server Standard FE		3	3,4	12,4	SUPERIOR	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	0	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

Server Sip-Quili -linux Ubuntu 12		3	2	8	ALTO	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	0	Robo de información	Herramientas maliciosas de entrega	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control remoto de maquinas infectadas- Establecer conexión externas	Ingeniería social- Phishing	Pérdida de integridad de datos
Software de Laboratorio Clinico	Examenes de pacientes	3	3,4	12,4	SUPERIOR	Footprinting -Escaneo de vulnerabilidades- Malware- Backdoor- Dispositivos infectados.- Recoleccion de credenciales de usuario.	0	Robo de información	0	Escalar privilegios- Ejecución de malware - Instalación y ejecución de programas en segundo plano- Control	Ingeniería social- Phishing	Pérdida de integridad de datos

										remoto de maquinas infectadas-Establecer conexión externas		
Software de Historias Clinicas	Registro de pacientes e historia clinica	3	3,4	12,4	SUPERIOR	Footprinting-Escaneo de vulnerabilidades-Malware-Backdoor-Dispositivos infectados.-Recoleccion de credenciales de usuario.	0	Robo de información	0	Escalar privilegios-Ejecución de malware-Instalación y ejecución de programas en segundo plano-Control remoto de maquinas infectadas-Establecer conexión externas	Ingeniería social-Phishing	Pérdida de integridad de datos

Ilustración 82. Activos con riesgos

A la lista de activos anteriomente identificados en la ilustración 82 se debe aplicar las buenas prácticas del ítem 3.2 y herramientas propuestas en ítem 3.3, para cada fase del ciclo de vida del APT según sus riesgos y amenazas para minimizar un ataque APT en una entidad hospitalaria.

Estas pruebas demuestran que el framework (marco de trabajo) tiene la función de un DLP, pero orientado a la parte humana, el cual se enfoca en que los administradores tengan una guía estratégica que gobierne sus activos sensibles a fuga de información y permita hacer gestión de la seguridad de ellos.

6.5. Anexo E. Análisis técnico generacion e implantación de malware.

Se utilizo el programa Poison IVY, para crear una muestra de malware, similar a la que usan los APT y que afectan los sistemas operativos identificados en el framework como sensibles a fuga de información, dicho malware se ocultara en un archivo .doc, el cual será enviado a la victima y ejecutara el malware, por motivos de seguridad solo se muestra algunos eventos de lo que sucede en caso de no seguir las recomendaciones y en caso de hacerlo.

Ejecuciòn de Poison IVY SOBRE un SERVIDOR cuyo sistema operativo es windows 8.

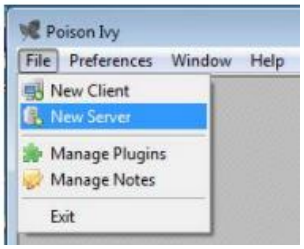


Ilustración 83.Ejecución de poison Ivy

Aplicación del parche para hacer el malware funcional sobre ambientes windows XP, windows server , windows 7 y 8.

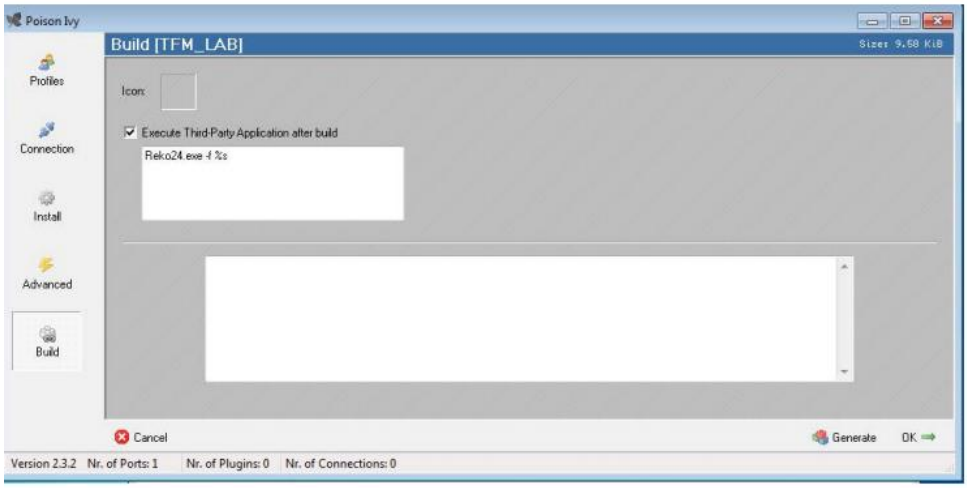


Ilustración 84. Aplicación de parche

Teniendo los sistemas antivirus actualizados, el encargado del área de sistemas tenía la oportunidad de detectar la muestra que genera POISON Ivy.

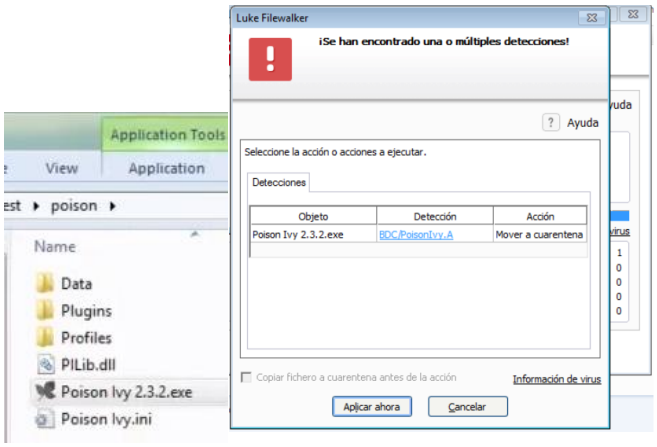


Ilustración 85.Detección de muestra con sistema antivirus actualizado

Archivo generado con destino a la víctima sin ocultar detectado por sistema Av.

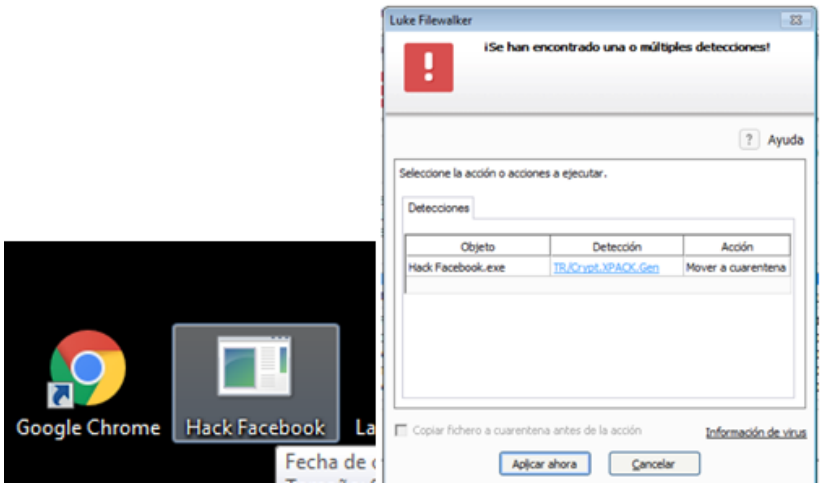


Ilustración 86.Muestra maliciosa detectada por sistema Av

Se oculta el malware para que sea indetectable por algunos sistemas con el programa open Cripter y themida.

Ilustración 87.Camuflage de muestra maliciosa

Al escanear el archivo camuflado con extensión.doc los antivirus no lo detectan y ya está listo para ser enviado a la víctima.

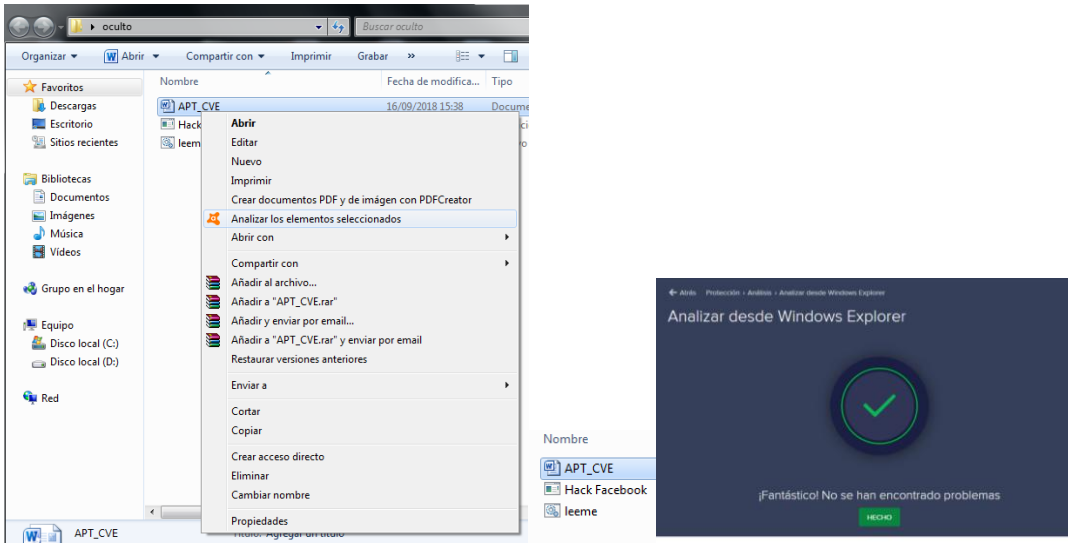


Ilustración 88. Resultado de escaneo de Archivo APT_CVE con malware oculto listo para enviar via correo.

Para evitar que pase esto es necesario en la entidad hospitalaria seguir las recomendaciones del anexo B y C, en la sección 6.3.1, donde se sigue dicha secuencia y en la sección 6.3 se proponen herramientas para evitarlo.

Ejecución de Poison Ivy desde la máquina de control si no se aplica recomendaciones, en el caso de la entidad tomada como modelo pasaría lo siguiente.

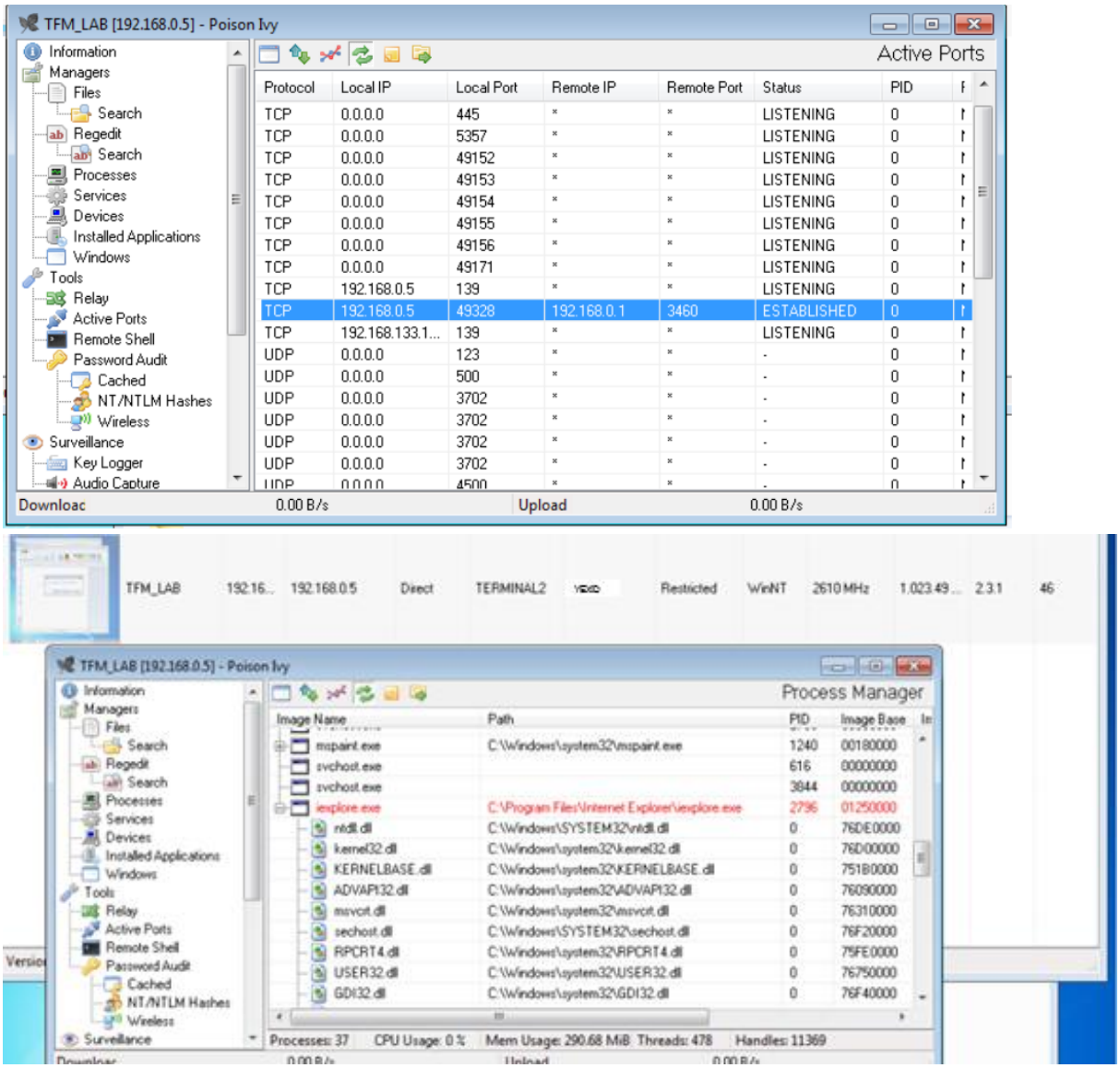


Ilustración 89.Conexión establecida con maquina victima

Es este caso ya el hacker tiene control de la máquina de la víctima, la cual ya está infectada y puede instalar nuevas herramientas de ataque lateral y que le permitan ocultar sus movimientos. Como también realizar otra serie de ataques para lograr el objetivo. Para saber como reaccionar ante estos sucesos remitase a resultados de objetivos 1,2,3 y 4 del trabajo de grado. Es importante saber que el eslabon mas débil son las personas y si no están capacitadas y tienen buenas prácticas como las propuestas en el framework, no habrá seguridad, asi se tengan los mejores sistemas en la organización.