ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD DE ASEGURAMIENTO LÓGICO EN ESTACIONES UTILIZANDO UN SOFTWARE DE PROTECCIÓN FINAL PARA UNA ENTIDAD FINANCIERA"

TRABAJO DE TITULACIÓN

Previa la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Alvaro Ernesto Padilla Vilema

GUAYAQUIL – ECUADOR

AÑO

2.018

AGRADECIMIENTO

Agradezco primeramente a Dios por su constante amparo, por las bendiciones diarias recibidas y amor infinito.

A mi padre por brindarme su apoyo en cada etapa de mi vida. A mi madre por inculcarme constancia, valentía frente a la vida y amor incondicional.

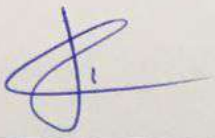
A mis hermanos por su calor fraterno y por ser el pilar fundamental en mi vida.

A mi tutor por su paciencia y apoyo para la culminación de este proyecto.

DEDICATORIA

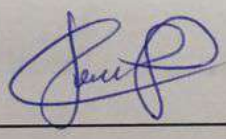
A Dios, a mis padres, a mis hermanos, maestros y amigos que estuvieron conmigo brindándome su apoyo durante mi etapa de posgrado.

TRIBUNAL DE SUSTENTACIÓN



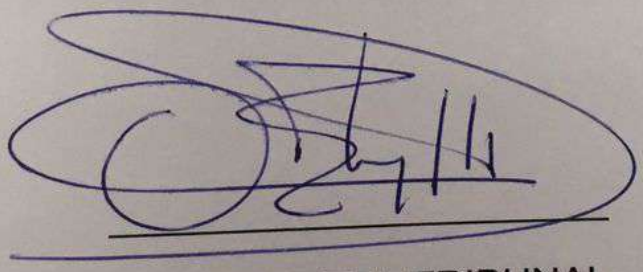
DIRECTOR MSIG/MSIA

MG. LENÍN FREIRE COBO



DIRECTOR DEL PROYECTO DE GRADUACIÓN

MG. JUAN CARLOS GARCÍA



MIEMBRO DEL TRIBUNAL

MG. OMAR MALDONADO DAÑÍN

DECLARACIÓN EXPRESA

"Declaro de forma expresa que todo el contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Alvaro Padilla V.

Alvaro Ernesto Padilla Vilema

RESUMEN

El objetivo de este proyecto es implementar un esquema de aseguramiento lógico en estaciones utilizando un software de protección final en una entidad financiera, de tal forma que se logre una mayor protección en las computadoras de la organización.

Para la implementación del esquema de seguridad se utilizará el software Symantec Endpoint Protection (SEP), el cual tiene 7 características de aseguramiento que nos ayudaran a minimizar las vulnerabilidades y amenazas que se presenten al momento de proteger la información sensible que maneja el usuario en sus labores diarias.

Entre las protecciones que se conseguirán con el uso del software SEP, se tienen las siguientes: análisis de comportamiento y reputación, ejecución de aplicaciones permitidas por la compañía, uso exclusivo de dispositivos permitidos, políticas de firewall, sistema de prevención de intrusiones.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Hoy en día uno de los principales objetivos en el que invierten las entidades financieras de mediano y gran tamaño es en posicionarse frente a la competencia utilizando los diferentes canales virtuales de atención a sus clientes. A partir del auge en el uso de las tecnología para realizar las diferentes transacciones y consultas sin la necesidad de ir a una entidad financiera, el sector bancario se ha vuelto un blanco apetecido por los delincuentes informáticos que de alguna u otra forma buscan robar información de los tarjetahabientes y dinero.

Los criminales informáticos están constantemente tratando de vulnerar los sistemas de protección de seguridad lógica de las instituciones, y para ello cada día generan mecanismos de intrusión y archivos maliciosos, los cuales generalmente son desplegados mediante correos electrónicos maliciosos o sitios web comprometidos hacia las estaciones de los usuarios de la empresa financiera.

Una vez que un equipo se encuentre comprometido, mediante técnicas de intrusión y despliegue, los programas maliciosos logran expandirse hacia las demás máquinas, consiguiendo un mayor campo de afectación. Secuestro de información, robo de información de tarjetahabientes, transferencias de dinero, daño a equipos sensibles, entre otros, son los daños y pérdidas que se tienen cuando un malware o virus avanzado ingresa a la red.

Por este motivo se ha considerado implementar un esquema de protección lógica para estaciones utilizando un software de protección final, el cual ayude en el aseguramiento de la infraestructura tecnológica.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

Hoy en día las entidades financieras buscan brindar mayor protección a sus clientes y colaboradores en el ámbito tecnológico, de tal forma que la información sensible y el dinero de sus usuarios se encuentren seguros. Se han conocido diferentes vectores de ataques dirigidos exclusivamente a los bancos, los cuales tienen como objetivo comprometer estaciones y servidores corporativos.

Ransomwares, malwares, troyanos, entre otros, están entre los ataques más conocidos por software de código malicioso, teniendo como objetivo secuestrar y/o robar información de las casas financieras. A fin de contrarrestar y mejorar el aseguramiento de los datos, en la actualidad se han desarrollado software que brindan una protección proactiva de punto final en los equipos.

En la implementación del esquema de aseguramiento lógico en estaciones, se busca proteger las diferentes capas vulnerables de un equipo, haciendo uso de las diferentes tecnologías que hoy en día ofrece un software de protección final.

Software y Hardware, cortafuego local, prevención de intrusos, entre otros, son parte de las respectivas fronteras que se aseguraran en los dispositivos finales, teniendo como un único objetivo, proteger el bien más preciado para toda organización: La Información.

1.2 DESCRIPCIÓN DEL PROBLEMA

En la actualidad las entidades financieras reciben un gran porcentaje de ataques de piratas cibernéticos comparado con otras industrias. Esto se debe, a que delincuentes todos los días están busca de información de clientes, contraseñas y dinero. El incremento de ataques dirigidos y las amenazas de día cero convierten a las estaciones de los usuarios en un blanco perfecto para ser atacados y conseguir información sensible.

Hoy en día, el banco ha tenido inconvenientes con ataques dirigidos cuyo foco son las estaciones de los usuarios, en las cuales se han insertado troyanos, software

malicioso, entre otros, logrando de esta forma comprometer información de la compañía y de clientes.

Existen alrededor de 3.200 computadoras, las cuales tienen instalado un antivirus cuyas configuraciones se encuentran por defecto, debido a que no existe una política integral que configure y administre la protección en dichas máquinas.

Actualmente no se está aprovechando en su totalidad el software instalado en los equipos, dado que solamente se tiene habilitada la protección basada en firmas, dejando de lado la protección basada en análisis de comportamiento, reputación de archivos, módulos de control de aplicaciones, dispositivos y host firewall.

Entre los incidentes más relevantes que se han suscitado, se pueden mencionar los siguientes:

- Alrededor de 30 estaciones y un servidor de archivos han sido comprometidos por software malicioso, los cuales han cifrado todos sus documentos, haciendo que los usuarios pierdan su información.

- Un ordenador fue detectado como miembro de una red infectada, el cual era controlado de forma remota, causando un excesivo consumo de ancho de banda, saturando el canal de Internet.

Al no contar con un correcto esquema de seguridad lógica en las estaciones, se tiene un riesgo latente muy alto, debido a que existen máquinas de usuarios que manipulan información sensible para la empresa, las cuales son vulnerables a los ataques de día cero.

1.3 SOLUCIÓN PROPUESTA

La propuesta consiste en implementar un esquema de aseguramiento lógico en estaciones utilizando un software de protección final, que permitirá tener una seguridad en los equipos de los usuarios mitigando vulnerabilidades, ataques de día cero y fugas de información.

En la actualidad el banco requiere proteger las estaciones de forma integral. Para ello se habilitarán las siguientes características que protejan las diferentes brechas de seguridad en las computadoras:

- Antivirus: Protección basada en firmas.
- Reputación de Archivos: Protección avanzada de archivos descargados.
- Análisis Comportamental: Protección para detectar amenazas en función de su comportamiento.
- Control de Aplicaciones: Protección para evitar la ejecución de aplicaciones no permitidas.
- Control de Dispositivos: Protección para el uso de dispositivos o medios extraíbles.
- Firewall Local: Protección para el tráfico malicioso entrante o saliente de las estaciones.

La correcta implementación del esquema permitirá asegurar la información que se encuentre en las estaciones debido a que las características mencionadas trabajan en conjunto y logran mitigar las vulnerabilidades que se presenten en los equipos.

Para la implementación del esquema de seguridad en estaciones se utilizará el software Symantec Endpoint Protection (SEP), debido a que el banco actualmente cuenta con licencias del producto.

SEP es un software de protección final que utiliza tecnologías avanzadas para mitigar amenazas y ataques de día cero, el cual se encuentra entre los tres principales “líderes” en protección de estaciones, según el cuadrante mágico de Gartner. [1]

Con la finalidad de cubrir las diferentes brechas de seguridad en las estaciones, se implementarán las siguientes características del producto:

- Protección en análisis de comportamiento y reputación.
- Control de aplicaciones y dispositivos.
- Módulo de firewall local.

1.4 OBJETIVO GENERAL

Implementar un esquema de aseguramiento lógico en estaciones utilizando un software de protección final para una entidad financiera.

1.5 OBJETIVOS ESPECÍFICOS

- Analizar la seguridad lógica actual en las estaciones de la empresa.
- Definir los componentes del esquema de seguridad lógica para las estaciones usando un software de protección final.
- Identificar los requerimientos y aplicativos que son de utilizados por los usuarios para realizar sus funciones.
- Analizar los servicios críticos que se pueden ver afectados por la habilitación de políticas restrictivas en las estaciones.
- Implementar un esquema de seguridad lógica para estaciones de trabajo usando un software de protección final.

- Comparar los resultados obtenidos entre la implementación del esquema de seguridad lógica propuesto y los resultados de los últimos 6 meses.

1.6 ALCANCE

- Explotar la herramienta SEP, debido que al momento no está siendo aprovechada en su totalidad.
- Implementar un esquema de seguridad que puede ser tomado como referencia para otras empresas.
- Reducir el riesgo de la perdida de información sensitiva.

1.7 METODOLOGÍA

Para definir un procedimiento a seguir en la implementación del esquema de aseguramiento lógico en las estaciones, se debe tomar en consideración indisponibilidad de los diferentes servicios que se ofrecen a los usuarios y clientes de la institución.

Para ello las diferentes características se habilitaran de forma progresiva, empezando por los módulos menos intrusivos para las estaciones. A continuación el orden de habilitación propuesto:

1. Protección de archivos mediante análisis de comportamiento y reputación.
2. Control de dispositivos.
3. Control de aplicaciones.
4. Módulo de firewall local.

La metodología de implementación de los diferentes módulos de SEP se basará en los puntos listados a continuación:

- Identificación de dispositivos de interfaz humano utilizado por los usuarios.
- Se realizará un levantamiento de aplicaciones que se encuentren instaladas en todas las estaciones de la empresa.
- Levantamiento de direcciones IPs y puertos utilizados por las diferentes aplicaciones cliente/servidor del banco.
- Análisis de Riesgo de indisponibilidad de servicios de aplicaciones críticas.
- Definición de proceso de revisión de software permitido e instalación.

Cabe indicar que al inicio de cada plan de trabajo se realizará un piloto en el cual involucre diferentes estaciones de diferentes áreas y cargos, esto con la finalidad de medir la afectación e incidencia por la habilitación de la respectiva característica habilitada.

CAPÍTULO 2

MARCO TEÓRICO

2.1 PROTECCIÓN DE ESTACIONES

En la actualidad es casi imposible no utilizar una computadora que no esté conectada a la red, ya sea a Internet o a una red privada, por lo cual es fundamental utilizar una estación que tenga las debidas protecciones ante las posibles amenazas que se encuentran en el medio.

Los atacantes crean programas maliciosos, tales como gusanos, virus, troyanos, que pueden comprometer los datos almacenados en el ordenador cliente, provocando el robo o la perdida de la información guardada. Dichos ataques

pueden provocar la indisponibilidad de los servicios hacia los clientes, pérdida de información privada y secretos corporativos, servir de punto medio para realizar ataques dirigidos hacia otros equipos. [2]

Para mejorar la protección de estaciones de trabajo, existen varias consideraciones que se deben implementar, tales como [3]:

- **Uso de firewall:** Ayuda a prevenir que conexiones no autorizadas se realicen en los equipos.
- **Instalación de antivirus:** Es un programa que ayuda a proteger los ordenadores de otros programas con código malicioso.
- **Uso de una cuenta con mínimos privilegios administrativos:** Una cuenta sin privilegios administrativos no permitirá que se realicen cambios en configuraciones y borrado archivos importantes, reduciendo de esta forma la efectividad de muchos virus.
- **Instalación de actualizaciones:** Se debe de realizar instalaciones de actualizaciones de forma periódica tanto a nivel de sistema operativo como de los aplicativos instalados, debido a que los atacantes constantemente están buscando nuevas formas de vulnerar los programas instalados.
- **Ingeniería Social:** Los usuarios deben de tener presentes los recursos, trucos o engaños que pueden utilizar los ciberdelincuentes para persuadir a sus víctimas, con la finalidad de que realicen ciertas actividades o compartan información para vulnerar la seguridad de los equipos.
- **Copias de Seguridad:** Si el usuario posee información sensitiva en su ordenador, es aconsejable que se realicen respaldos periódicos de los datos almacenados, debido a que en el caso de que los archivos se encuentren infectados por algún virus, se pueda restaurar los mismos, minimizando de esta forma los daños ocasionados.

2.2 PROTECCIÓN DE ANTIVIRUS

La protección de antivirus en un equipo consiste en identificar y bloquear la ejecución de programas maliciosos mediante el uso de un aplicativo denominado “antivirus”, salvaguardando de esta forma la información almacenada los diferentes equipos. [4]

Los antivirus buscan patrones basados en firmas de algún programa malicioso ya conocido. Al ser una protección basada en firmas, existe una dependencia en que el fabricante publique constantemente nuevas definiciones para que los ordenadores tengan las últimas versiones de definiciones aplicadas.

Hoy en día por la robustez de los programas de código malicioso, los antivirus están utilizando diferentes tecnologías de detención para contrarrestar las diferentes amenazas de forma proactiva, debido a que la protección reactiva basada en firmas constantemente esta un paso atrás porque los virus pueden ir mutando y contagiando estaciones antes de ser detectados por las definiciones descargadas en los equipos. [5]

2.3 PROTECCIÓN PROACTIVA

La protección proactiva es un complemento de la protección basada en firmas, dado que los métodos de detección de esta protección son basados en análisis heurísticos y análisis comportamental.

La Real Academia Española define el término “heurístico” como la manera de buscar la solución de un problema mediante métodos no rigurosos, como por tanteo, reglas empíricas, etc. [6]

Los antivirus en la actualidad están utilizando la heurística para determinar si un fichero desconocido que tiene un comportamiento sospechoso puede ser un elemento de alto o bajo riesgo para la estación [7]. Los análisis heurísticos en un antivirus operan por medio de su base de reglas, comparando el contenido del archivo con variables que indican si el mismo es un posible archivo malicioso.

2.4 CONTROL DE APLICACIONES Y DISPOSITIVOS

Los controles de aplicaciones y dispositivos son características de los software de protección final, que ayudan a reforzar el aseguramiento en las estaciones y detener una posible infección por algún programa de código malicioso. Dichas características son parte del software Symantec Endpoint Protection - SEP. [8]

Entre los controles que se pueden implementar con las directivas de control de aplicaciones y dispositivos se tienen:

- Permitir o denegar la ejecución de aplicaciones definidas por la empresa.
- Permitir, Bloquear o terminar la ejecución de un proceso, archivo o ejecutable.
- Controlar el acceso al registro del sistema.
- Control sobre un comportamiento anómalo a nivel de archivos de Office y PDF.
- Bloquear el acceso a scripts y archivos con extensiones específicas.
- Permitir o bloquear el acceso a ficheros y aplicativos usando su valor de hash.
- Bloquear ataques desde dispositivos extraíbles.
- Habilitar dispositivos USB de interfaz humana utilizados en el corporativo.
- Administra los periféricos que pueden conectarse las estaciones.

2.5 MODULO DE FIREWALL LOCAL

Un firewall local tiene como función principal proteger y administrar las conexiones entrantes y salientes de un equipo [9]. Las reglas definidas en una política de firewall se basan en tres características tales como conexiones, dispositivos y comunicaciones [10].

- **Conexiones:** Una de las primeras acciones que se debe tener en consideración al definir una regla de firewall es definir si la conexión se debe "permitir" o "bloquear". Adicional a ello se debe identificar la dirección del flujo de la conexión, dado que se puede tener comunicaciones "entrantes", "salientes" o "entrantes y salientes".

  Las conexiones entrantes permiten la comunicación desde otro equipo hacia el equipo local. Por el contrario una conexión saliente permite el flujo desde el equipo local hacia otro equipo. Un tráfico entrante y saliente, permite un flujo bidireccional de las conexiones.

- **Dispositivos:** Como segundo consideración se debe especificar cuáles son los equipos o dispositivos que se deben aplicar la regla de firewall implementada. Se puede considerar como un equipo una dirección URL, una dirección IP, un rango de direcciones IPs o un segmento de red.
- **Comunicaciones:** Como último paso en la implementación de una regla de firewall se debe definir los protocolos de comunicación tales como TCP, UDP, ICMP, o todos.

  Al momento de seleccionar los protocolos se debe especificar los puertos asociados a dichos protocolos, los cuales pueden ser puertos conocidos,

puertos específicos o un rango definido por la aplicación que genera dicho tráfico.

Finalmente se deben identificar los puertos habilitados para la comunicación, como locales o remotos. Un puerto es definido como local cuando recibe conexiones entrantes, por el contrario un puerto se lo define como remoto cuando el mismo genera conexiones salientes.

2.6 APLICATIVOS INTERNOS

Una de las primeras tareas de los ordenadores y aplicaciones informáticas fue automatizar los cálculos y procesos de productividad que ayuden a las empresas a simplificar el trabajo manual operativo realizado. [11]

Se define como una aplicación interna a una herramienta informática específica de una compañía, la cual ayuda a los empleados en los diferentes procesos de negocio y aplicaciones de sistemas de información [12]. Las aplicaciones internas generalmente están alineadas a los objetivos del negocio de cada empresa, dado que es gracias a ellas que los empleados incrementan su nivel de productividad y eficiencia.

2.7 DISPOSITIVOS USADOS EN ENTIDADES FINANCIERAS

Los dispositivos usados en entidades financieras al igual que sus aplicaciones internas van orientados a reducir las tareas manuales y operativas de los empleados. [12]

En una entidad financiera existen dispositivos específicos utilizados en sus actividades diarias las cuales están conectados a los diferentes estaciones de los usuarios, tales como pantallas táctiles de turnos para auto atención, máquinas

contadoras de billetes y monedas, equipos detectores de billetes falsos, procesadores de cheques, cámaras para reconocimiento facial, lectores de firmas, máquinas impresoras de tarjetas, entre otros dispositivos.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1 INTRODUCCIÓN

La entidad financiera en la cual se implementará el esquema de protección lógico de estaciones, es una de las más grandes instituciones bancarias de país en la actualidad, motivo por el cual en ocasiones previas ha recibido varios ataques dirigidos por ciberdelincuentes, los mismos que tienen por objetivo robar información valiosa de usuarios/clientes y dinero.

Como en toda compañía los usuarios utilizan sus estaciones para desempeñar sus actividades diarias, en las cuales manejan información sensible para la empresa, ya sean datos de clientes, usuarios o tarjetahabientes. Dicha información puede

encontrarse en los documentos alojados en los discos locales de los equipos, servidores de archivos, aplicativos, buzón de correo, o red interna.

En la actualidad la empresa tiene como directiva para sus usuarios, que todo documento con información sensible sea almacenado en los servidores de archivos, los cuales cuentan con un sistema de respaldo periódico y de aseguramiento, garantizando de esta forma la confiabilidad, disponibilidad e integridad de la información. Sin embargo diariamente los usuarios manejan archivos temporales y de seguimiento de actividades los cuales podrían ser unos de los principales objetivos de los delincuentes informáticos al momento de infectar una estación final.

Hoy en día la entidad cuenta con un aproximado de 3.200 estaciones de usuarios, en las que en ciertas máquinas por más de 15 ocasiones han sido infectadas con virus de ataque de día cero, secuestrando de esta forma información y documentos alojados en dichos equipos.

A continuación se detalla el vector de infección realizado por el software malicioso:

1. Como primer paso el usuario de la empresa recibe un correo cuyo remitente es de una dirección desconocida con un documento adjunto de tipo .doc o .pdf.
2. El usuario pensando que es un requerimiento de algún cliente, descarga y abre el documento recibido, infectando de esta forma el equipo del usuario, dado que el software malicioso viene oculto en el adjunto recibido.
3. Una vez que la estación se encuentra infectada, el virus se comunica con su servidor central en Internet, a fin de obtener la información necesaria para la activación del mismo.

4. Posterior al paso previo, el virus empieza a cifrar de forma silenciosa todo el contenido alojado en el disco duro de la máquina.
5. Al culminar el cifrado de la información, el virus presenta un mensaje al usuario, informando que los archivos del equipo se encuentran cifrados y que para la recuperación de los mismos, se debe pagar un rescate por la información durante un tiempo establecido.
6. Si otros equipos consumen recursos del equipo infectado (unidades de red, carpetas compartidas o archivos), pueden verse también afectados por el virus, debido a que uno de los puertos por el cual se propaga es el TCP 455.

En las ocasiones que se han detectado este tipo de infecciones, el usuario es quien ha reportado a la mesa de ayuda, indicando que ha recibido cierto mensaje en su equipo y que no puede abrir ningún de sus archivos.

La mesa de ayuda realiza el escalamiento de la novedad al área de Infraestructura y Seguridades, la cual realiza el procedimiento de aislamiento y recopilación de hallazgos en el equipo, con la finalidad de desinfectar el equipo.

Al analizar el equipo con una herramienta adicional al antivirus, se logra identificar los posibles archivos maliciosos que se encuentran en dicha máquina, los cuales son subidos al sitio web del antivirus, esto con el objetivo de que se generen firmas de protección para dicha variante de virus, debido a que la base de firmas hasta ese momento no las contiene.

El proceso de generación de nuevas firmas por parte del fabricante de antivirus, puede tomar hasta un lapso de 8 horas para publicación de la remediación, tiempo en cual más máquinas pueden verse afectadas por el archivo malicioso recibido en sus correos.

Debido al tiempo y dependencia en la generación de nuevas firmas, es necesario implementar una protección proactiva, que nos ayude en el aseguramiento lógico de las estaciones.

3.2 LEVANTAMIENTO DE REQUERIMIENTOS

Actualmente la entidad financiera analizada, cuenta con licencias disponibles del antivirus Symantec Endpoint Protection, por lo cual se utilizará dicho software de protección para el aseguramiento lógico de las estaciones.

El esquema de aseguramiento lógico en estaciones consta de la habilitación y afinamiento de cada característica de SEP, a fin de cubrir las diferentes brechas de seguridad en los equipos. A continuación las características que se habilitarán:

- Protección Antivirus.
- Control de Aplicaciones y Dispositivos.
- Protección Firewall Local.
- Directivas de Cumplimiento.

Figura 3.1: Esquema Seguridad Lógica Estaciones

La correcta habilitación de las funcionalidades indicadas previamente sin la afectación de los servicios a los usuarios, depende básicamente del levantamiento de información que se realice en las estaciones de los usuarios. A continuación se detallarán los diferentes requerimientos necesarios para el esquema de aseguramiento lógico, los cuales servirán de insumos para la configuración de las directivas de control:

- **Requerimientos para protección de archivos**

  Actualmente la protección de archivos en base a firmas del antivirus se encuentra habilitada en las computadoras, por lo que es válido conocer la configuración actual a fin de realizar los respectivos ajustes y de esta forma implementar una protección proactiva.

- **Requerimientos para control de aplicaciones y dispositivos**

  Las características de control de ejecución aplicaciones y dispositivos no están activas en los equipos de los usuarios, por lo cual es importante conocer las aplicaciones permitidas por la empresa, el estándar de aplicaciones instaladas en los equipos dependiendo del cargo de usuario, los dispositivos de interfaz humana permitidos, los usuarios que tienen acceso a medios extraíbles.

- **Requerimiento para firewall local**

  La protección del firewall local en las estaciones se encuentra instalada pero no configurada, por lo que se considera que dicha protección no está activa. Para la generación de las diferentes reglas de tráfico se debe conocer todas las comunicaciones que se generan por las aplicaciones cliente - servidor que son consumidas por los usuarios en los equipos.

3.3 APLICACIONES INTERNAS INSTALADAS

La entidad financiera posee el área llama Organización y Métodos, la cual tiene como uno de sus objetivos definir el respectivo estándar de los programas y aplicativos internos instalados en las computadoras del corporativo mediante la identificación del cargo de los colaboradores y sus funciones realizadas.

A continuación se listan los respectivos aplicativos internos, software y utilitarios permitidos, los cuales se permitirán en la directiva de control de aplicaciones:

Tabla 3.1: Listado de aplicativos internos de la empresa

Software Instalado	Tipo Aplicativo
ACL for Windows	Aplicativo Tercero
ADAM	Aplicativo Interno
AdminReglaNegocio.exe	Aplicativo Interno
Adobe Acrobat	Utilitario
Adobe Acrobat Profesional	Utilitario
Adobe Creative Suite 6 Master Collection	Utilitario
Adobe Flash	Utilitario
Adobe Help Manager	Utilitario
Adobe Illustrator	Utilitario
Adobe Reader	Utilitario
Agentes de SCCM	Aplicativo Tercero
Altitude	Aplicativo Interno
ARIS	Aplicativo Tercero
AutoCAD	Utilitario
Autodesk	Utilitario
AutoFacil	Aplicativo Interno
BridgerInsight	Aplicativo Interno
Cheqscan	Aplicativo Interno
Compresor 7-Zip	Utilitario
Conexión a Escritorio remoto	Utilitario
Conexión del proyector del directorio	Aplicativo Tercero
Conexión y revisión de informes médicos con el IESS	Aplicativo Tercero
Cupos de Anticipos y Préstamos	Aplicativo Interno

Software Instalado	Tipo Aplicativo
Data Dynamics	Aplicativo Interno
DHL Connect	Aplicativo Tercero
Digital Watchdog	Aplicativo Tercero
DIMM	Aplicativo Tercero
Echelon (Monitoreo ATMs)	Aplicativo Interno
Editor Texto – Notepad ++	Utilitario
Ejecutable utilizado para imprimir desde IE	Aplicativo Interno
Ejecutable utilizado por CheqScan	Aplicativo Interno
Ejecutables utilizados por IE	Aplicativo Interno
Equitrac	Aplicativo Interno
Ergo IBV	Aplicativo Interno
ERP	Aplicativo Interno
evolution reporter	Aplicativo Interno
Extreme SNA	Aplicativo Interno
Finanware	Aplicativo Interno
Firmar electrónicamente los DOCs BCE	Aplicativo Tercero
FnwCliFragmento	Aplicativo Interno
fnwCliTipoC	Aplicativo Interno
fnwSop (Application Proxy)	Aplicativo Interno
FnwSopSeguridad (Application Proxy)	Aplicativo Interno
FnwTabla9 (Application Proxy)	Aplicativo Interno
fnwTablas11 (Application Proxy)	Aplicativo Interno
FnwVaRGenerador (Application Proxy)	Aplicativo Interno
FnwVaRGeneral (Application Proxy)	Aplicativo Interno
FnwVaRProcesar (Application Proxy)	Aplicativo Interno
FnwVaRReporte (Application Proxy)	Aplicativo Interno
FortiClient	Aplicativo Tercero
Genera Token para acceder al site MasterCard	Aplicativo Tercero
HIS	Aplicativo Interno
HRDP Remote	Aplicativo Interno
Hyland	Aplicativo Interno
IBM SPSS	Aplicativo Interno
InterfaseDiaria	Aplicativo Interno
Internet Explorer	Utilitario
Java	Utilitario
K-Lite Codec Pack	Utilitario
Kofax	Aplicativo Interno
LMS(Claves Desechables ATMs)	Aplicativo Interno

Software Instalado	Tipo Aplicativo
Lync Basic 2013	Utilitario
Micro Focus Rumba	Aplicativo Interno
Monitor Plus	Aplicativo Interno
MS Framework	Utilitario
MS Office Professional Plus 2016	Utilitario
MS Office Project Professional 2016	Utilitario
MS Silverlight	Utilitario
MS SQL	Utilitario
Multicheque	Aplicativo Interno
NeoTeller	Aplicativo Interno
Odawin	Aplicativo Interno
Onbase	Aplicativo Interno
Oracle Crystal	Aplicativo Interno
Panini	Aplicativo Interno
Panini Multicheques	Aplicativo Interno
pmcrypto	Aplicativo Interno
pmFirmaElectronica	Aplicativo Interno
PowerTools	Utilitario
RASplus	Aplicativo Interno
Reporteador Hyland	Aplicativo Interno
RStudio	Aplicativo Tercero
SafeNet (software aduana)	Aplicativo Tercero
Sentinel	Aplicativo Interno
Sentinel Cumplimiento y Riesgo	Aplicativo Interno
SEP - Antivirus	Utilitario
Skype Empresarial	Utilitario
Softphone 3CXPhone	Aplicativo Tercero
Sumadora Virtual	Aplicativo Interno
SX Virtual Link	Aplicativo Tercero
Syscards	Aplicativo Interno
TechMaster	Aplicativo Tercero
Turbo Switf	Aplicativo Interno
Turnero KTQMA	Aplicativo Interno
Utilitario Fatca	Aplicativo Interno
ValidarArchivos	Aplicativo Interno
Visioneer	Aplicativo Tercero
Web Deployment Tool	Aplicativo Tercero
WinSCP	Aplicativo Tercero

3.4 DISPOSITIVOS DE INTERFAZ HUMANA UTILIZADOS

Hoy en día los dispositivos de interfaz humana que utilizan los colaboradores, realizan tareas operativas que ayudan en la atención ágil hacia los clientes de la entidad bancaria. Dichos dispositivos en su mayoría tiene una conexión de tipo USB hacia las estaciones, por lo que permitir el uso de dichos dispositivos especiales con las directivas actuales, sería habilitar el acceso total a los puertos USB, generando riesgo de un posible robo de información o un medio de infección de infección por virus.

El área de Seguridad de la información de la empresa ha recopilado por medio de sus diferentes funciones el listado de dispositivos especiales que ciertos usuarios tienen acceso, los cuales más adelante se permitirán en la directiva de control.

Tabla 3.2: Dispositivos de Interfaz Humana - USB utilizados

DISPOSITIVO	IDENTIFICADOR FÍSICO DEL DISPOSITIVO
Panini - IMPRESORA	Class: 219179a1-5ef7-476b-87de-de13ed8fc50c
Panini E172976	Device: USB\VID_121F&PID_0010\6&66CA680&1&5
Panini Ensobradora Multi CH 01	Device: USB\VID_121F&PID_0001\6&66CA680&1&1
Panini Ensobradora Multi CH 02	Device: USB\VID_121F&PID_0002\6&66CA680&1&1
OLIVETTI	Device: USBPRINT\OLIVETTIIBM_PPII\8&2EE63A16&0&USB001
USB Receiver	Class: 4d36e97e-e325-11ce-bfc1-08002be10318
WinUSB_DeviceLlavesDesechables	Class: c49068c2-b65c-4de2-83d9-d4b945aa5c91
USB DisplayLink Adapter	Class: 3376f4ce-ff8d-40a2-a80f-bb4359d1415c
PinClienteUSB	Device: USB\VID_2332&PID_2333\805513022B28
BCE Token	Class: 50dd5230-ba8a-11d1-bf5d-0000f805f530
BCE Token 1	Class: db4f6ddd-9c0e-45e4-9597-78dbbad0f412
ProxCard SegFisica	Class: 4d36e978-e325-11ce-bfc1-08002be10318

CAPÍTULO 4

ANÁLISIS DE RIESGOS EN AFECTACIÓN DE SERVICIOS

4.1 SITUACIÓN ACTUAL

Las estaciones de los colaboradores durante mucho tiempo han sido el eslabón olvidado dentro de las recomendaciones de seguridad de la información, motivo por el cual han sido muy vulnerables. Posterior a los primeros ataques dirigidos de código malicioso recibidos, se ha realizado un levantamiento de información de la situación actual de las computadoras, encontrando de esta forma las siguientes falencias que pueden ser aprovechadas por los atacantes informáticos:

- Equipos sin protección de antivirus.
- Antivirus con políticas por defecto.
- No existe un estándar de aplicaciones instaladas.
- Programas de punto a punto instalados.
- Falta de administración del firewall local.
- Ausencia de control sobre los medios conectados extraíbles permitidos.
- Usuarios con privilegios administrativos sobre los equipos.
- Carencia de puntos de restauración.
- No se tiene un plan de instalación de actualizaciones computadoras.

Equipos sin protección de antivirus: Se identificó que en la infraestructura de la compañía existe un diecisiete por ciento de los equipos sin el antivirus instalado, haciendo de esta forma más vulnerable la red.

Tabla 4.1: Equipos sin antivirus instalado

Tipo de Versión	Cantidad
Estaciones con antivirus	2.772
Estaciones sin antivirus	478
TOTAL	**3.200**

Antivirus con políticas por defecto: La consola de administración de los clientes de Symantec tiene vinculadas a ciertos contendores de estaciones, las políticas por defecto que se generan al momento de la instalación, las cuales no son recomendadas por el fabricante debido a su permisividad. En el siguiente gráfico se listan con contenedores de estaciones que tienen vinculadas dichas directivas:

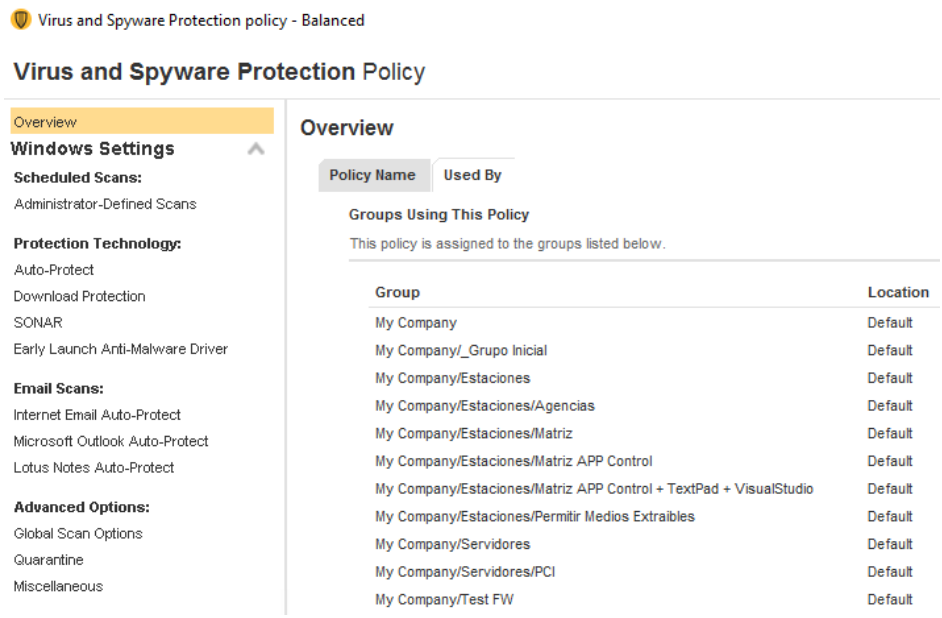


Figura 4.1: Política de antivirus por defecto aplicada a las estaciones

No existe un estándar de aplicaciones instaladas: Mediante un inventario del software instalado en las computadoras de los colaboradores, se ha identificado que existen programas posiblemente maliciosos que pueden servir como una puerta trasera para que los ciberdelincuentes ingresen a la infraestructura. Entre los programas más relevantes no permitidos se tienen los siguientes:

Tabla 4.2: Programas no permitidos instalados en estaciones

Software Posiblemente Malicioso	Cantidad
Antivirus no permitidos	**61**
avast! Free Antivirus	1
AVG 9.0	3
AVG PC TuneUp 2014	2
AVG PC TuneUp 2015	2
AVG Security Toolbar	9
Malwarebytes' Anti-Malware	29
McAfee Security Scan Plus	12
Panda ActiveScan 2.0	1
Panda Cloud Cleaner	2

Software Posiblemente Malicioso	Cantidad
Juegos	**3**
FIFA 10	1
Sopa de Letras 2.1	1
Sopa de Letras 2.5.0	1
P2P	**42**
Ares 2.0.9	1
Ares 2.1.7	2
Ares 2.1.8	4
Ares 3.1.6.3040	2
Ares 3.1.7.3042	2
aTube Catcher	6
aTube Catcher versión 3.8	3
eMule Acceleration Tool	1
FinalTorrent 2011	17
shARES Toolbar	3
uTorrentBar_ES Toolbar	1
Total general	**106**

Programas punto a punto instalados: Los programas punto a punto o mejor conocidos como P2P son utilizados para compartir archivos. Mediante el inventario de software instalado en las estaciones, se ha identificado que los usuarios utilizan dichos programas para descargar músicas y videos e internet, y con esta acción la descarga de posibles virus informáticos.

Falta de administración del firewall local: El rol del firewall local de las estaciones se encuentra habilitado en el cliente de antivirus. Sin embargo el mismo no está configurado, debido a que tienen directivas que permite todo el tráfico entrante y saliente desde las computadoras. En la siguiente gráfica se muestra la directiva por defecto que permite todo el tráfico de todas las aplicaciones (regla número 24):

SEP12 Estaciones - Politica de Firewall

Firewall Policy

Rules

Rules | Notifications

Inherit Firewall Rules from Parent Group

...	Enabled	Name	Action	Application	Host	Service
18	✔	Permitir LLMNR de tráfico ipv6	Allow	Any	Any	UDP:[Local=5355]
19	✔	Permitir detección de servicios web desde dir...	Allow	Any	Remote:10... Remote:17... Remote:19... Remote:16...	UDP:[Local=3702]
20	✔	Bloquear detección de servicios web	Block	Any	Any	UDP:[Local=3702]
21	✔	Permitir SSDP desde direcciones IP privadas	Allow	Any	Remote:10... Remote:17... Remote:19... Remote:16...	TCP:[Local=2869]
22	✔	Bloquear SSDP	Block	Any	Any	TCP:[Local=2869]
23	✔	Permitir ping, pong y tracert	Allow	Any	Any	ICMP:[Type=0; Incoming] ICMP:[Type=8] ICMP:[Type=11; Incoming]
24	✔	Permitir todas las aplicaciones	Allow	*	Any	Any
25	✔	Permitir GYESIS01	Allow	Any	Local:GYE...	Any

Figura 4.2: Política de antivirus por defecto firewall estaciones

Ausencia de control sobre los medios conectados extraíbles permitidos: Actualmente los medios extraíbles son permitidos o bloqueados por una directiva de grupo configurada a nivel de los controladores de dominio, la cual no tiene un control o una segregación al momento de la habilitación de dispositivos con conexión a puertos USB, ya sean estos periféricos o dispositivos de interfaz humanada dedicados para el negocio.

Usuarios con privilegios administrativos sobre los equipos. : Se ha identificado que de las 3.200 estaciones que se tienen activas en la empresa, en 1953 estaciones tienen configurados a usuarios finales como administradores de las computadoras, por lo que dichos usuarios poseen control total administrativo sobre su estación de trabajo, pudiendo instalar programas, cambiar configuración, etc.

Tabla 4.3: Estaciones con administradores locales no permitidos

	Total equipos	Equipos sin Adm. Locales	Equipos con Adm. Locales
Estaciones de trabajo	3.200	1.247	1.953

Carencia de puntos de restauración: En la actualidad no se tiene una directiva que administre los puntos de restauración en las estaciones, debido a que los mismos ocupan espacio considerable en los discos de las mismas. Sin embargo un punto de restauración es uno de los medios que se tiene para recuperar la información posterior a una infección por un virus informático.

No se tiene un plan de instalación de actualizaciones computadoras: Las estaciones, posterior a su instalación no reciben actualizaciones de seguridad, debido a que la empresa no tiene un plan continuo de instalación de parches que permita instalar los boletines publicados por el fabricante.

4.2 ANÁLISIS DE SERVICIOS CRÍTICOS QUE SE PUEDEN AFECTAR POR LA HABILITACIÓN DE POLÍTICAS RESTRICTIVAS DE APLICACIONES

Las directivas de control de aplicaciones si bien es cierto serán aplicadas sobre todas las aplicaciones instaladas en las estaciones de trabajo, en esta sesión se identificarán las aplicaciones sobre las cuales se deben tener mucha más consideración al momento de la implementación debido a su criticidad.

La compañía mediante la disponibilidad de sus servicios, ha definido ciertas aplicaciones y sistemas que no pueden verse afectados, debido a que los mismos son herramientas fundamentales al momento de la atención de los clientes.

A continuación se indicarán y detallarán los aplicativos de escritorio que tienen un nivel de criticidad alta, debido a que al verse afectados, podrían incidir la disponibilidad de los servicios que ofrece el banco a sus clientes:

- Neo Teller
- Gestor Documental
- Syscard Debit
- Cliente OnBase
- CRM
- Altitude
- Extreme SNA

Neo Teller: Aplicativo cliente servidor, el cual permite a los cajeros en ventanillas visualizar e imprimir las cartolas con los saldos de los clientes. El aplicativo se encuentra instalado en la ruta c:\Neoteller* y c:\Plantillas*.

Gestor Documental: Aplicativo cliente servidor, cuya función es visualizar y mostrar todos los documentos que un cliente tenga registrados en la entidad financiera, ya sean estos C.I., papeleta de votación, planillas de servicios básicos, pasaporte, etc. El aplicativo se encuentra instalado en la ruta c:\Program Files\Gestor Documental*.

Syscard Debit: Aplicativo cliente servidor, el cual permite administrar la información relacionada a las tarjetas de débito de los clientes. El aplicativo se encuentra instalado en la ruta c:\Program Files\TechSoft\Syscard Debit*.

Cliente OnBase: Aplicativo cliente servidor, cuya función principal es la digitalización de los documentos presentados por los clientes, cabe indicar que posterior a la digitalización, dichos archivos serán gestionados por el Gestor Documental. El aplicativo se encuentra instalado en la ruta c:\Program Files\Hyland\OnBase Client*.

CRM: Es un aplicativo con interfaz web, cuya función principal es procesar las solicitudes de los clientes de la entidad financiera referentes a: consultas, requerimientos o reclamos se administran en el sistema. El aplicativo no posee ruta de instalación, dado que es consumido mediante un navegador.

Altitude: Aplicativo cliente servidor, el cual permite a los agentes del área de call center contestar las llamadas realizadas por los clientes. El aplicativo se encuentra instalado en la ruta c:\Program Files\Altitude*.

Extreme SNA: Es un aplicativo cliente servidor, el cual permite ingresar y realizar las diferentes transacciones referentes a los productos que ofrece la empresa a sus clientes. El aplicativo se encuentra instalado en la ruta c:\Program Files\AlexSoft S.A\Extreme SNA 2016*.

Las diferentes rutas en donde se encuentran alojadas las aplicaciones críticas para la atención a los clientes, serán permitidas en las directivas de control de aplicaciones debido a la sensibilidad de las mismas.

4.3 ANÁLISIS DE SERVICIOS CRÍTICOS QUE SE PUEDEN AFECTAR POR LA HABILITACIÓN DE POLÍTICAS RESTRICTIVAS DE FIREWALL

En esta sección se detallarán las conexiones que tienen las aplicaciones críticas para la atención hacia los clientes indicadas en la sección anterior, debido a que las políticas restrictivas de firewall controlan las comunicaciones habilitadas o permitidas en las estaciones de trabajo.

Tabla 4.4: Servicios Críticos de la empresa

Aplicativo	Origen	Destino	Puerto Destino
Neo Teller	Estaciones de Usuarios	Servidores NeoTeller	443
Gestor Documental	Estaciones de Usuarios	Servidores GestorDoc	8080
Syscard Debit	Estaciones de Usuarios	Servidores SysCards	8704
Cliente OnBase	Estaciones de Usuarios	Servidor OnBase01	9443
CRM	Estaciones de Usuarios	Servidores CRM	80
Altitude	Estaciones de Usuarios	Servidores Altitude	7443
Extreme SNA	Estaciones de Usuarios	Servidores Extreme	5443

Todas las comunicaciones indicadas en la tabla de conexiones anterior, tienen como origen las estaciones de los usuarios debido a que es desde este equipo donde se están consumiendo las aplicaciones. Los destinos hacia donde se comunican las estaciones son los servidores de los diferentes aplicativos, los cuales están escuchando por sus respectivos puertos TCP indicados en la tabla.

CAPÍTULO 5

IMPLEMENTACIÓN DEL ESQUEMA DE PROTECCIÓN LÓGICA EN ESTACIONES UTILIZANDO SEP

Una vez definidos y establecidos los servicios críticos de la entidad financiera, en las siguientes secciones se procederá a detallar las políticas y los respectivos controles que ayudaran a mitigar las vulnerabilidades encontradas en la revisión de la situación actual de la compañía.

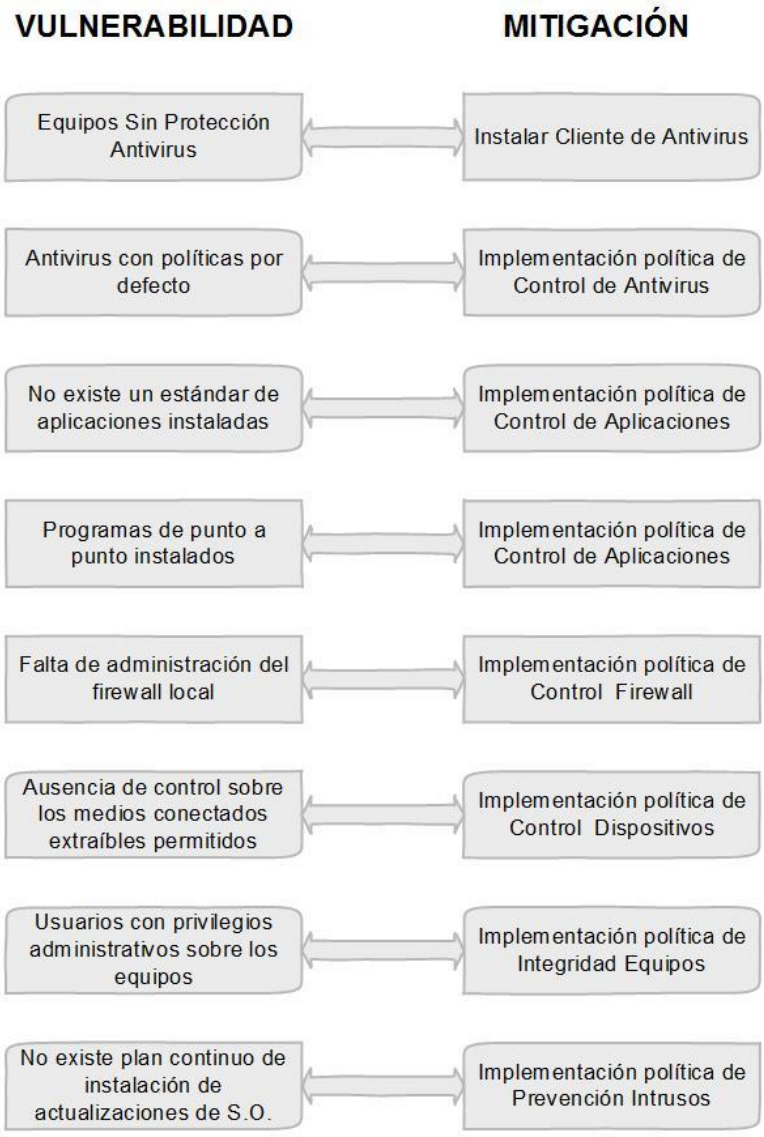


Figura 5.1: Esquema de Remediación de Vulnerabilidades Encontradas

5.1 FASES DEL PLAN DE IMPLENTACIÓN

La implementación del esquema a de aseguramiento lógico en estaciones se ha divido en tres fases, las cuales constan en la elaboración y afinamiento de cada característica de SEP, a fin de cubrir las diferentes brechas de seguridad en los equipos. A continuación las fases a implementar:

- **Fase 1:**
  - ✓ **Protección Antivirus:** Protección basada en firmas.
  - ✓ **Reputación de Archivos:** Protección avanzada de archivos descargados.
  - ✓ **Análisis Comportamental:** Protección para detectar amenazas en función de su comportamiento.

- **Fase 2:**
  - ✓ **Control de Aplicaciones:** Protección para evitar la ejecución de aplicaciones no permitidas.
  - ✓ **Control de Dispositivos:** Protección para el uso de dispositivos o medios extraíbles.

- **Fase 3:**
  - ✓ **Protección Firewall Local:** Protección para el tráfico malicioso entrante o saliente de las estaciones.
  - ✓ **Prevención de Intrusos:** Protección capaz de analizar los diferentes patrones de un ataque mediante el análisis de los paquetes de red.

Cada fase será implementada de forma independiente y en tiempos diferentes con el objetivo de que en caso que hubiese algún tipo de inconveniente, se pueda solventar la novedad en menor tiempo.

5.2 CREACIÓN DE POLÍTICAS DE ANTIVIRUS EN SEP

Las directivas de SEP correspondientes al módulo de protección antivirus y spyware, para la detección programas con código malicioso, tienen las siguientes características:

Tabla 5.1: Características de la directiva de antivirus

CARACTERÍSTICAS	OPCIONES
Auto protección del sistema de archivos	Análisis de todos los archivos en busca de virus y riesgos de seguridad. Limpia o pone en cuarentena los archivos infectados según corresponda. Registra los archivos maliciosos al momento del arranque del equipo. Notifica al usuario del equipo en caso que hubiera algún riesgo de seguridad detectado.
Auto protección de email	Escanea todos los archivos adjuntos en un correo, incluyendo los comprimidos. Limpia o pone en cuarentena los archivos infectados según corresponda. Notifica al usuario del equipo en caso que hubiera algún riesgo de seguridad detectado en un archivo adjunto.
Sonar	Las detecciones heurísticas de alto riesgo se ponen en cuarentena. Se registran todas las detecciones heurísticas de bajo riesgo. Detecta los archivos con un comportamiento sospechoso.
Administración de escaneos	Se puede programar escaneos activos todos los días, dependiendo de la definición. Se analizan todos los archivos y carpetas, incluidos los archivos comprimidos. Escanea la memoria, las ubicaciones de infección común y los lugares conocidos de riesgo de virus y seguridad. Limpia los archivos infectados por virus.

En la entidad financiera analizada se ha definido la política de protección de virus en todas las estaciones, siguiendo las mejores prácticas indicadas por el fabricante (Symantec). [13]

La directiva de SEP correspondiente al módulo de “Protección Virus y Spyware”, se la ha definido y configurado a nivel de la consola de admiración antivirus, la misma que tiene las siguientes características:

Administración de Escaneo

- **Escaneo Diario**

  Todos los días a las 12 pm se realiza un escaneo rápido, en la cual se analiza todos los archivos y procesos que se tiene en memoria, así mismo los archivos que se encuentran en los directorios temporales, archivos comprimidos, entre otros. Cabe indicar que el escaneo se lo realiza en dicho horario debido a que es un horario de bajo impacto para los usuarios.

Tabla 5.2: Configuración de Escaneos Diarios

Administración de escaneos	Alta Seguridad
Escaneo Diario	Habilitado, cada día a las 12:00 PM
Tipo de escaneo	Escaneo Activo
Tipos de archivos	Escanear todos los archivos (Bloqueado)
Características de Escaneo: Memoria…	Si
…rutas comunes de infección	Si
…virus conocidos y rutas de alto riesgo de seguridad	Si
Escaneo de archivos comprimidos	Si, 3 niveles al interno
Migración / copia de Almacenamiento	Omitir archivos fuera de línea y dispersos
…abrir archivos con respaldo	No
Abrir archivos con sincronización	Si
Nivel de Insight	Nivel 5 (Típico)
Acción de Insight	Cuarentena/Solo registrar (Registrar en log)

Administración de escaneos	Alta Seguridad
Detecciones de reputación de Insight: 1ra acción / 2da acción(si la 1ra falla)	Cuarentena/Solo registrar (Registrar en log)
Programación	Diariamente a las 12:30AM
Duración del escaneo	Escanee hasta 2horas
Aleatorizar la hora de inicio del escaneo	Si
Reintento del escaneo	Sí, dentro de las 72 horas
Detecciones de malware: 1ra acción / 2da acción(si la 1ra falla)	Limpiar/Cuarentena
Virus: Anular acciones configuradas para malware?	No
Detecciones de Riesgos de Seguridad: 1ra acción / 2da acción(si la 1ra falla)	Cuarentena/Solo registrar(registrar en log)
Adware: ¿Anular las acciones configuradas para los riesgos de seguridad?	No
¿Herramienta de intrusión?	No
¿Aplicaciones Engañosas?	No
¿Control Parental?	No
¿Acceso Remoto?	No
¿Riesgos de Seguridad?	No
¿Spyware?	No
¿Trackware?	No
Respaldar los archivos antes de iniciar la reparación	Si
Terminar los procesos automáticamente	Si
Detener los servicios automáticamente	Si
Mostrar una notificación en caso de que al computadora se encuentre infectada	No

- **Escaneo Completo**

Un escaneo completo consiste en analizar todas las unidades de disco que se encuentran en las estaciones, el cual se ejecuta todos los días viernes a las 13:00. Cabe indicar que el escaneo se lo realiza en dicho horario debido a que es un horario de bajo impacto para los usuarios y se lo realiza una sola vez a la semana debido al consumo de recurso que utiliza en las estaciones.

Tabla 5.3: Configuración de Escaneos Completos

Administración de escaneos	Alta Seguridad
Configuraciones de escaneo Completos definidas por el administrador	Habilitado, cada Viernes a las 1:30 PM
Escaneo de las siguientes carpetas	Todas las carpetas
Tipos de archivos	Escanear todos los archivos
Características de Escaneo: Memoria…	Si
…rutas comunes de infección	Si
…virus conocidos y rutas de alto riesgo de seguridad	Si
Escaneo de archivos comprimidos	Si, 3 niveles de profundidad
Migración / copia de Almacenamiento	Omitir archivos fuera de línea y dispersos
…abrir archivos con respaldo	No
Abrir archivos con sincronización	Mejor rendimiento de aplicaciones
Habilitar la búsqueda de la reputación de archivos	Habilitado
Nivel de Insight	Nivel 5 (Típico)
Detecciones de reputación de Insight: 1ra acción / 2da acción(si la 1ra falla)	Cuarentena/Solo registrar (solo a log)
Detecciones de malware: 1ra acción / 2da acción(si la 1ra falla)	Limpiar/Cuarentena
Virus: Anular acciones configuradas para malware?	No
Detecciones de Riesgos de Seguridad: 1ra acción / 2da acción(si la 1ra falla)	Cuarentena/Solo registrar (solo a log)
Adware: ¿Anular las acciones configuradas para los riesgos de seguridad?	No
Terminar los procesos automáticamente	Si
¿Spyware?	Si

Tabla 5.4: Configuración avanzada de escaneos completos

Administración de escaneos	Alta Seguridad
Administer-Defined Scans, Advanced Tab	N/A
Retrasar los escaneos programados cuando las laptops estén consumiendo energía de la batería	Si
Permitir que los escaneos se ejecuten tanto si un usuarios se encuentra o no logoneado	Si
Mostar notificaciones de detección cuando los usuarios se encuentran logoneados	Si
Permitir que los escaneos de inicio se ejecuten cuando el usuario inicia sesión	No
Ejecutar un escaneo activo cada vez que el equipo tome nuevas definiciones	Si
Mostrar el progreso del escaneo	No

Auto Protección de SEP

La autoprotección es la primera protección que ofrece el cliente de SEP, el cual nos cubre de alguna infección en tiempo real. La autoprotección se habilita cuando se está copiando, abriendo, comprimiendo archivos, entre otras opciones. Como una de las características principales, se tiene contempla la configuración de las diferentes acciones que se pueden realizar al detectar un archivo malicioso.

Tabla 5.5: Configuración de Auto Protección

Auto-Protección	Alta Seguridad
Habilitado	Si (Bloqueado)
Tipos de archivos	Escanear todos los archivos (Bloqueado)
Escaneo de archivos comprimidos	Si (Bloqueado)
Bloquee los riesgos de seguridad de ser instalado	Si (Bloqueado)
Escaneo de archivos en computadoras remotas...	Si (Bloqueado)
...escaneo de archivos remotos solo cuando se ejecutan archivos	Si (Bloqueado)
Archivos de confianza en computadoras remotas que ejecutan auto-protección	Si (Bloqueado)

Tabla 5.6: Configuración avanzada de Auto Protección

Auto-Protección	Alta Seguridad
Habilitar el cache en la red	Sí; eliminar las entradas después de 600 segundos (Bloqueado)
Virus: ¿Anular acciones configuradas para malware?	Archivo es accedido o modificado (Bloqueado)
Escanear cuando un archivo es respaldado	Si (Bloqueado)
No escanear archivos cuando ejecutan procesos seguros	Si (Bloqueado)
Comprobar los disquetes para identificar virus de arranque, cuando se accede a dichos dispositivos	Si (Bloqueado)
Acción a tomar cuando se encuentra el virus de arranque de disquete	Solo registrar (solo a log)
Incluso si la acción es 'Deje solo (solo registro)': ¿eliminar virus recién creado?	Si (Bloqueado)
... ¿eliminar los riesgos de seguridad recién creados?	No (Bloqueado)
Detecciones de malware: 1ra acción / 2da acción(si la 1ra falla)	Limpiar/Cuarentena (Bloqueado)
Virus: ¿Anular acciones configuradas para malware?	No (Desbloqueado)
Detecciones de Riesgos de Seguridad: 1ra acción / 2da acción(si la 1ra falla)	Cuarentena/Borrado (Bloqueado)
¿Herramienta de intrusión?	No (Bloqueado)
¿Aplicaciones Engañosas?	No (Desbloqueado)
¿Riesgos de Seguridad?	No (Desbloqueado)
Terminar los procesos automáticamente	Si (Bloqueado)
Detener los servicios automáticamente	Si (Bloqueado)
Mostrar una notificación en caso de que al computadora se encuentre infectada	Si (Bloqueado)
¿Cuándo carga la protección automática?	Cuando el equipo inicia (Bloqueado)
Chequear los discos cuando la computadora se apague	Si (Bloqueado)
Habilitar caché de archivos …	Si, (Bloqueado)
... volver a explorar el caché cuando lleguen nuevas definiciones	Si (Bloqueado)
…monitoreo de las sesión de red cada X milisegundos	Si, cada 1000 ms (Bloqueado)

Descarga de Protección - Insight

La descarga de protección de Insight se activa cuando el cliente de SEP no encuentra en su base local de firmas, la reputación del archivo que está analizando en ese momento. Para realizar esta descarga, las estaciones requieren de acceso a las direcciones de Symantec en internet.

El nivel de sensibilidad que se tiene configurado para dar como malicioso es de 5, configuración típica, debido a que si se aplica una configuración más restrictiva, de incrementa el número de falsos positivos reportados por la herramienta.

Tabla 5.7: Configuración Descarga de Protección - Insight

Descargas de Protección Insight	Alta Seguridad
Habilitar la descarga de Insight	Si (Bloqueado)
Nivel se sensibilidad de los archivos maliciosos	5 (Típico) (Bloqueado)
… también detectar archivos con X o menos usuarios	No (Bloqueado)
… también detectar archivos conocidos por los usuarios X o menos días	No (Bloqueado)
Automáticamente asegurar cualquier archivo descargado de un sitio de intranet	Si (Bloqueado)
Detección de descargas maliciosas: primera acción ...	Cuarentena (Bloqueado)
… si la primera acción falla	Solo registrar (registrar a log) (Bloqueado)
Acción para archivos no probados	Mostrar(Bloqueado)
Mostar las notificaciones de Insight en una computadora infectada	Si (Bloqueado)

SONAR

La característica de SONAR tiene como función examinar el comportamiento de los aplicativos y procesos para decidir si las mismas son maliciosas. Entre las principales configuraciones en esta característica es que si SONAR detecta un alto

riesgo lo envía a cuarentena. Así mismo por el contrario, si detecta un bajo riesgo simplemente lo registra a nivel de los eventos.

Tabla 5.8: Configuración de SONAR

SONAR	Alta Seguridad
Habilitar SONAR	Si (Bloqueado)
Acción de detección de alto riesgo	Cuarentena (Bloqueado)
Acción de detección de bajo riesgo	Log (Bloqueado)
Habilitar el modo agresivo	No (Bloqueado)
Mostrar alerta de detección	Si (Bloqueado)
Preguntar antes de finalizar un proceso	No (Bloqueado)
Preguntar antes de detener un servicio	No (Bloqueado)
Acción a tomar cuando se detecta cambios a nivel del DNS	Bloquear (Bloqueado)
Acción a tomar cuando se detecta el cambio del archivo de hosts	Bloquear (Bloqueado)
Comportamiento sospechoso Acción de detección de alto riesgo	Bloquear (Bloqueado)
Comportamiento sospechoso Acción de detección de bajo riesgo	Ignorar (Bloqueado)
Configuración del cliente heredado de TruScan	
Escanea troyanos y gusanos…	Si (Bloqueado)
... usa valores predeterminados de sensibilidad de troyano / gusano definidos por Symantec	Si (Bloqueado)
Escanea keyloggers...	Si (Bloqueado)
... usar los valores predeterminados de sensibilidad de keylogger definidos por Symantec	Si (Bloqueado)
Cuando se detecta un keylogger comercial	Log (Bloqueado)
Cuando se detecta una aplicación comercial de control remoto	Log (Bloqueado)
Con qué frecuencia debe ejecutar TruScan?	A una frecuencia de escaneo personalizada; escanea procesos cada 15 minutos, escanea nuevos procesos inmediatamente (Bloqueado)

Vinculación de la nueva directiva de antivirus

Para la vinculación y masificación de la nueva política de protección de antivirus, se la debe realizar de forma controlada, a fin de no causar afectación en los usuarios, para lo cual se ha definido la vinculación en las siguientes fases:

- **Fase Piloto**: Habilitar las nuevas configuraciones en la política "SEP Estaciones - Política de Antivirus y Antispyware - High Security" y vincular dicha directiva al contenedor "Piloto" (el contenedor tiene estaciones puntuales).

Figura 5.2: Contenedor Estaciones - Fase Piloto

- **Fase Tecnología**: Vincular la política al contenedor "Tecnología y DO", en el que se encuentran estaciones de usuarios correspondiente al área de tecnología.

Figura 5.3: Contenedor Estaciones - Fase Tecnología & DO

- **Fase Estaciones Área Comercial**: Vincular la política al contenedor "Testing", el cual contendrá estaciones del área comercial y cajas a fin de probar el piloto.

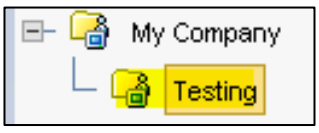


Figura 5.4: Contenedor Estaciones - Fase Testing

- **Fase de Masificación**: Finalmente vincular en todos los contenedores de estaciones la política “SEP Estaciones - Nueva Política de Antivirus y Antispyware”, los cuales se listan en la siguiente captura.

This policy is assigned to the groups listed below.

Group	Location
My Company/Estaciones/AGENCIA/Ag. Remigio Crespo	Default
My Company/Estaciones/AGENCIA/Ag. Ventanas	Default
My Company/Estaciones/Agencias/SEP 12	Default
My Company/Estaciones/DATACARD	Default
My Company/Estaciones/Infraestructura	Default
My Company/Estaciones/Matriz/SEP 12	Default
My Company/Estaciones/Matriz APP Control/SEP 12	Default
My Company/Estaciones/Permitir Medios Extraibles/Desktop	Default
My Company/Estaciones/Permitir Medios Extraibles/Laptop	Default
My Company/Estaciones/Permitir Medios Extraibles/Temporal	Default
My Company/Estaciones/Piloto Desarrollo	Default
My Company/Estaciones/Test	Default
My Company/Estaciones/TESTING	Default
My Company/Estaciones/TESTING/Sucursal Cuenca	Default

Figura 5.5: Listado de Contenedores Estaciones

5.3 CREACIÓN DE POLÍTICAS DE APLICACIONES EN SEP

Las políticas de control de aplicaciones están compuestas por un sin número de reglas de protegen a los aplicativos, ya sea permitiendo o bloqueando la ejecución de ciertos programas, la escritura o modificación de archivos específicos, el acceso a claves de registro, entre otras acciones. Para ello se han definido las siguientes reglas de control que formaran parte de la directiva de control:

- Bloquear la ejecución de aplicaciones no permitidas.
- Bloquear por hash la ejecución de archivos maliciosos reportados.

- Proteger archivos Office y Adobe.
- Bloquear la ejecución de programas desde medios removibles.
- Impedir la creación de la carpeta RECYCLER.
- Bloquear el acceso al Autorun.inf.
- Proteger los archivos del cliente y claves de registro.

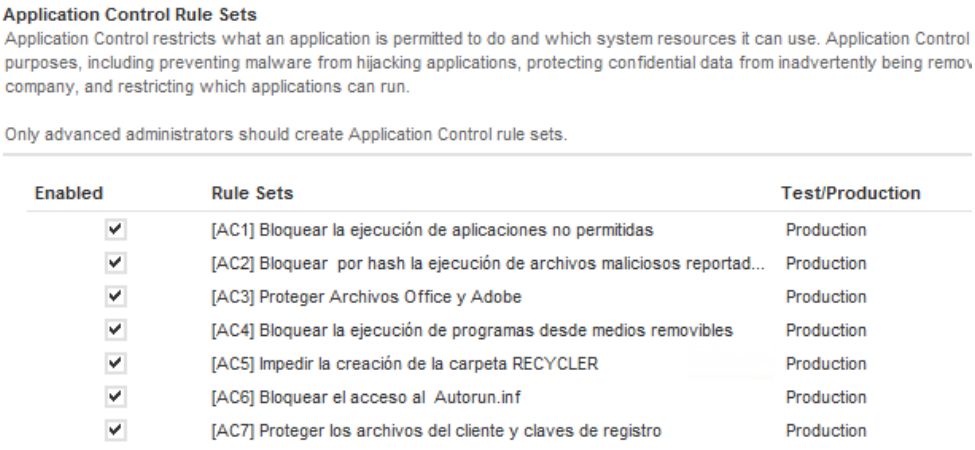


Figura 5.6: Reglas configuradas en la directiva de control de apps

- **Bloquear la ejecución de aplicaciones no permitidas:** Mediante una lista blanca de aplicaciones permitidas, se permite la ejecución de exclusivamente dicho software detallado, y a su vez bloqueando todo lo que no forme parte de dicho listado.

  La lista permitida está compuesta por las rutas de instalación en donde se alojan los archivos EXE de los aplicativos.

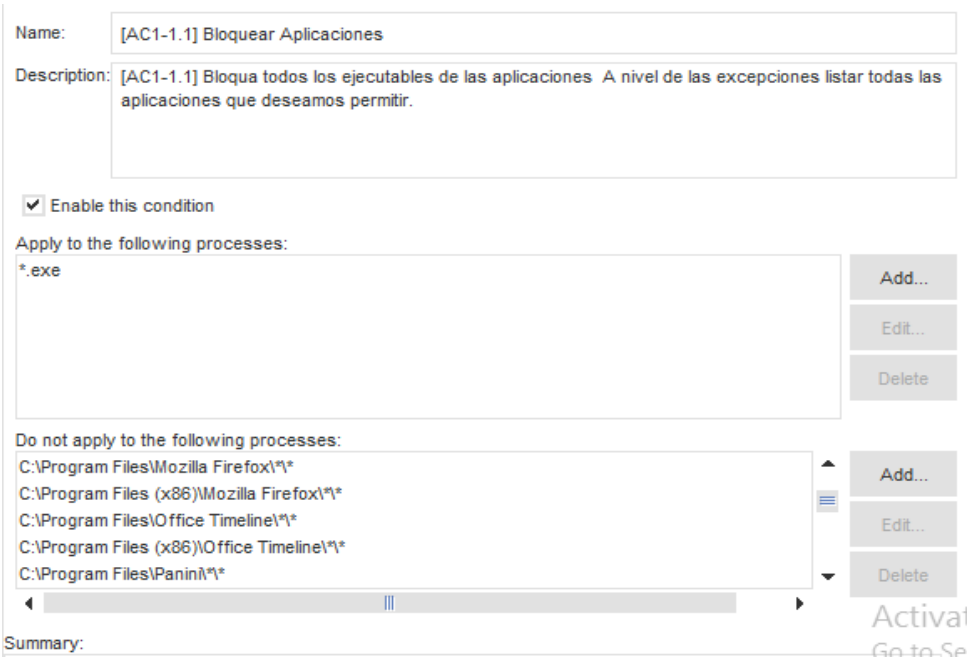


Figura 5.7: Regla de control de ejecución de aplicaciones

Las aplicaciones permitidas que forma parte de la directiva se la obtuvo mediante el levantamiento de información realizado por el área de Organización y Métodos de la empresa, debido a que entre unas sus funciones es definir el estándar de uso de aplicaciones del banco.

Tabla 5.9: Regla de Bloqueo de aplicaciones no permitidas

REGLA	REGLA INTERNA	PROCESO O RUTA SOBRE EL CUAL SE TOMA DESCISIÓN	ACCIÓN
Bloquear la ejecución de aplicaciones no permitidas Procesos: * **Excepciones:** Ninguna	Bloquear aplicaciones no permitidas	Rutas de Ejecutables bloqueadas: * Rutas de Ejecutables Excepcionadas: C:\Program Files\AhnLab** C:\Program Files (x86)\AhnLab**" "C:\Program Files\Altitude** "C:\Program Files\ARIS7.0** c:\program files\aris express** c:\program files\aris7.2** C:\Program Files (x86)\aris7.2**" ***Se detallan todas las ruta permitidas en la tabla de aplicaciones permitas.**	Bloquear Acceso Ejecución

A continuación se listan las aplicaciones con los respectivos directorios que se encuentran permitidas en la regla:

Tabla 5.10: Listado Aplicaciones Permitidas en la directiva

Aplicación Permitida	Ruta Instalación
Antivirus Symantec	C:\ProgramFiles\Symantec\Symantec Endpoint Protection**
7-Zip	C:\Program Files\7-Zip**
Adobe Flash	%SystemRoot%\System32\Macromed\Flash
Adobe Reader	C:\Program Files\Adobe** C:\Program Files (x86)\Common Files\Adobe** C:\Program Files\Common Files\Adobe**
Java	C:\Program Files\Java**
MS Framework	C:\Windows\Microsoft.NET**
Skype Empresarial	Ya excluido dentro de Office
MS Office	C:\Program Files\Microsoft Office**
Internet Explorer	C:\Program Files\Internet Explorer**
Agentes de SCCM	C:\Windows\CCM**
	C:\Windows\ccmcache**
	C:\Windows\ccmsetup**
SO	C:\Windows\SysWOW64**
	C:\Windows\System32**
SO	C:\Program Files\Microsoft Policy Platform**
SO	C:\Program Files\Common Files**
SO	C:\Program Files\Windows Media Player**
SO	C:\Program Files\Realtek**
3CXPhone	C:\Program Files\3CXPhone**
7-Zip	C:\Program Files\7-Zip\
Adobe Acrobat	C:\Program Files (x86)\Adobe\Acrobat Reader DC\
Adobe Acrobat Profesional	C:\Program Files\Adobe
Adobe Creative Suite 6 Master Collection	C:\Program Files\Adobe
Adobe Flash	C:\Windows\system32\Macromed\Flash\
Adobe Help Manager	C:\Program Files (x86)\Adobe\
Adobe Illustrator	c:\Program Files\Adobe\Adobe Illustrator CS2\
Adobe Reader	C:\Program Files\Adobe\Reader 11.0\Reader\
AhnLab Online Security	C:\Program Files\AhnLab**
Altitude	C:\Program Files\Altitude**
ARIS	C:\Program Files\ARIS7.0** C:\program files\aris express**

Aplicación Permitida	Ruta Instalación
AutoCAD	C:\Program Files\Autodesk\AutoCAD 2016\
Autodesk	C:\Program Files\Autodesk**
AutoFacilBG	C:\Program Files\AutoFacilBG**
Cheqscan	C:\Pogram Files\cheqscan**
	C:\Program Files (x86)\cheqscan**
	C:\pm_image**
	C:\Imagenes Cheques
Chrome	C:\Program Files\Google\Chrome**
Cupos de Anticipos y Préstamos	C:\Program Files\NuevosCuposAnticiposyPrestamos**
Digital Watchdog	C:\Program Files\Digital Watchdog**
Equitrac	C:\Program Files\Equitrac**
Extreme SNA	C:\Program Files\AlexSoft S.A**
Herramientas MS SQL Server 2005 Express Edition	C:\Program Files\Microsoft SQL Server\
HIS	C:\Program Files\Microsoft BizTalk Adapters for Host Systems 2.0**
Hyland	C:\Program Files\Hyland**
InterfaseDiaria	C:\Program Files\InterfaseDiaria**
Internet Explorer	C:\Program Files\Internet Explorer**
Java	C:\Program Files\Java\
K-Lite Codec Pack	C:\Program Files\K-Lite Codec Pack**
Kofax	C:\Program Files\Kofax**
Lync Basic 2013	C:\Program Files (x86)\Microsoft Office\
Micro Focus Rumba	C:\Program Files\Micro Focus**
Microsoft Office Access database engine 2007	C:\Program Files (x86)\Microsoft Office\
Mozilla Firefox	C:\Program Files\Mozilla Firefox**
MS Framework	C:\Windows\Microsoft.NET\Framework\
MS Lync 2013	C:\Program Files\Microsoft Lync**
MS Office	C:\Program Files (x86)\Microsoft Office\
MS Office Professional Plus 2013	C:\Program Files (x86)\Microsoft Office\
MS Silverlight	C:\Program Files\Microsoft Silverlight**
MS SQL	C:\Program Files\Microsoft SQL Server**
NeoTeller	C:\NeoTeller** C:\Plantillas**
Office Timeline	C:\Program Files\Office Timeline**
Onbase	C:\Program Files\Hyland\OnBase Client\

Aplicación Permitida	Ruta Instalación
Panini	C:\Program Files\Panini** C:\Program Files\WELLS FARGO\Panini Scanner Driver**
QuickTime	C:\Program Files\QuickTime**
SafeNet	C:\Program Files\SafeNet**
Sumadora Virtual	C:\Program Files\Banco Guayaquil\Sumadora Virtual**
Techsoft	C:\Program Files\Techsoft** C:\Syscards\Win**
ValidarArchivosBG	C:\Program Files\ValidarArchivosBG**
Visioneer	C:\Program Files\Visioneer**
WinSCP	C:\Program Files\WinSCP**
ACL for Windows	C:\Program Files\ACL Software\ACL for Windows 12**
ADAM	C:\Program Files\ADAM Technologies**
CutePDF	C:\Program Files\Acro Software\CutePDF Writer**
Data Dynamics	C:\Program Files\Data Dynamics\ActiveReports Pro**
DHL Connect	C:\Program Files\DHL Connect**
DIMM	C:\SRI-DIMN-2017**
Ergo IBV	C:\Program Files\IBV**
Evolution reporter	C:\evolution** \\gyerrhhdb01\evolution$*\
Finanware	C:\Program Files\FinanWare Reporte**
FnwCliFragmento	C:\Program Files\ComPlus Applications**
FortiClient	C:\Program Files\Fortinet\FortiClient**
HRDP Remote	C:\Program Files\Honeywell\HRDP**
Monitor Plus	C:\Program Files\Plus TI\Monitor Plus**
Oracle Crystal	C:\Program Files\Oracle\Crystal Ball**
pmcrypto	C:\Program Files\pmarket\pmcrypto**
pmFirmaElectronica	C:\Program Files\Plan Market\pmFirmaElectronica**
PowerTools	C:\Program Files\Visioneer**
RASplus	C:\RASplus**
Sentinel Cumplimiento y Riesgo	C:\Program Files\SmartSoft\Sentinel Cumplimiento Riesgo** C:\SmartSoft\Sentinel Cumplimiento y Riesgo**
Sentinel	C:\Program Files\SmartSoft\Sentinel Prevention**
SmartViewer	C:\Program Files\Samsung\SmartViewer3.0**
SX Virtual Link	C:\Program Files\silex technology\SX Virtual Link** C:\Users\Public\GestorDocumental\imagenes**
TechMaster	C:\Program Files\TechMaster Setup** C:\Program Files\TechMaster Audit**
Web Deployment Tool	C:\Program Files\IIS\Microsoft Web Deploy**
Odawin	C:\Program Files\SeventeenMile\Odabank Win**
Panini Multicheques - Drivers	C:\Program Files\PR2_ToolKit+**

- **Bloquear por hash la ejecución de archivos maliciosos reportados:** La regla tiene como objetivo bloquear por hash los ejecutables maliciosos publicados en los boletines de seguridad cuando se tiene una amenaza de día cero.

  Constantemente el área de Seguridad de la Información reporta a Tecnología los ejecutables con su respectivo hash MD5 o SHA256, los cuales son agregados para evitar que en el caso de que ingresen a las estaciones no puedan ejecutarse.

Figura 5.8: Regla de Bloqueo de archivos maliciosos por hash

Tabla 5.11: Detalle regla de bloqueo de archivos maliciosos por hash

REGLA	REGLA INTERNA	PROCESO O RUTA SOBRE EL CUAL SE TOMA DESCISIÓN	ACCIÓN
Bloquear por hash la ejecución de archivos maliciosos reportados Procesos: * Excepciones: Ninguna	Bloquear estas aplicaciones MD5	• c3626fb922d1836b6ce68465bc45 • 5cc47fe6a6e5b84e5d0e70218258 • 12bc9fcd7f59bd4a0c0477ccbaghj • 645d1dfb0715e483e4f3e341c355 • a7df539598aadf1d40fe79bdcc174 • a7df539598aadf1d40fe32bdcc714 • f97d2e6f8d820dbd3b66f237d4f09 • 84c82835a5d21bcf75a706d8a549 • 7bf2b57f2a205768755cf238fb32cc • 05da32043b1e3a47de63450f954d	Bloquear Acceso Ejecución

- **Proteger archivos Office y Adobe:** Esta regla tiene como objetivo salvaguardar todos los archivos Office y Adobe que se encuentren alojados en los equipos, mediante el análisis de los procesos que editan ó modifican dichos ficheros, protegiendo e esta forma que los mismos no sean modificados por aplicaciones maliciosas.

  Se han definido los procesos y aplicativos que pueden tener acceso de edición a dichos ficheros, entre los cuales se tienen procesos de la suite de Office (EXCEL.EXE, WINWORD.EXE, OUTLOOK.EXE), ejecutable de Adobe, entre otros.

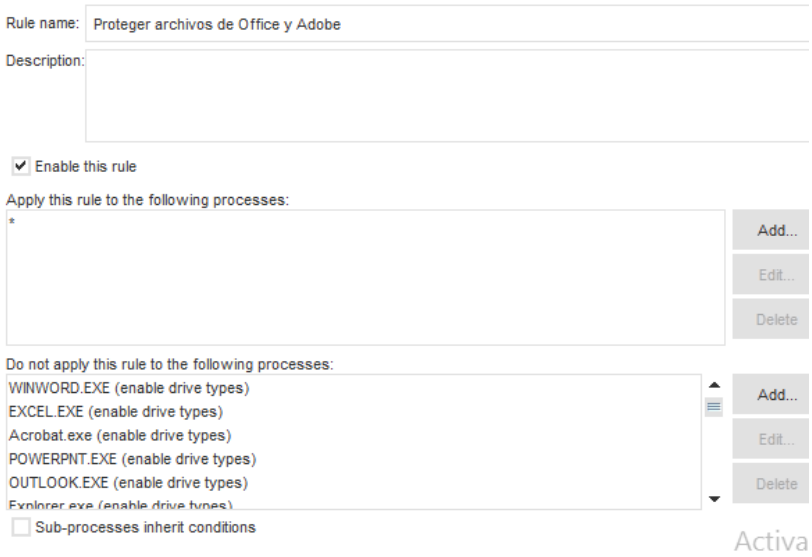


Figura 5.9: Regla de control apps - Proteger archivos Office y Adobe

Tabla 5.12: Detalle regla proteger archivos Office y Adobe

REGLA	REGLA INTERNA	PROCESO O RUTA SOBRE EL CUAL SE TOMA DESCISIÓN	ACCIÓN
Proteger Archivos Office y Adobe **Procesos: *** **Excepciones:** • WINWORD.EXE • EXCEL.EXE • Acrobat.exe • POWERPNT.EXE • OUTLOOK.EXE • Explorer.exe • iexplore.exe • chrome.exe • mstsc.exe • AcroRd32.exe • Skydrive.exe • VISIO.EXE • ONENOTE.EXE	Proteger Archivos de Office y Adobe	• ****.docx • ****.xls • ****.doc • ****.xlsx • ****.pdf • ****.ppt • ****.pptx	Bloquear Acceso de Modificación

- **Bloquear la ejecución de programas desde medios removibles:** Esta regla bloqueará la ejecución de cualquier programa que se ejecute desde medios removibles, incluyendo: unidades flash USB, unidades de CD/DVD y otras unidades tales como unidades Zip y Jazz.

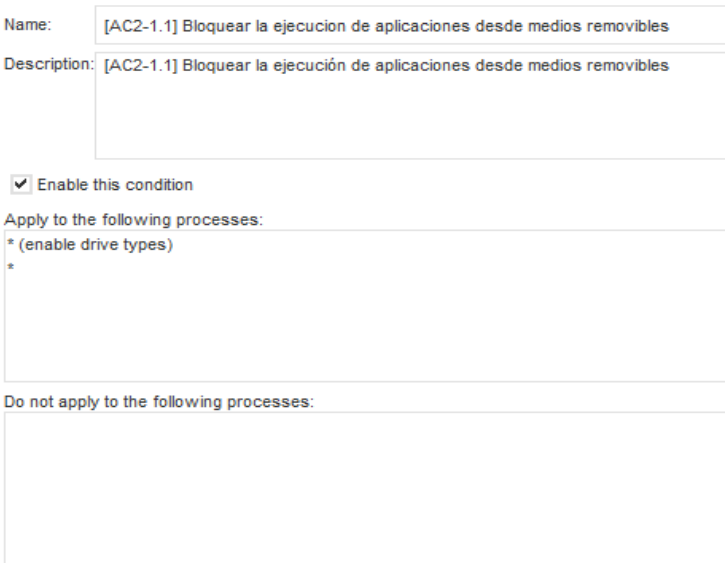


Figura 5.10: Bloquea Ejecución Programas en Medios Removibles

Tabla 5.13: Detalle regla bloqueo ejecución Programas en Medios Removibles

REGLA	REGLA INTERNA	PROCESO O RUTA SOBRE EL CUAL SE TOMA DESCISIÓN	ACCIÓN
Bloquear la ejecución de programas desde medios removibles **Procesos:** * **Excepciones:** Ninguna	Bloquear la ejecución de aplicaciones desde medios extraíbles	• * (enable drive types) • *	Bloquear Acceso de Ejecución

- **Impedir la creación de la carpeta RECYCLER:** Esta regla de control de aplicaciones tiene como objetivo evitar la creación de la carpeta RECYCLER provocado por un programa malicioso.

Figura 5.11: Impedir la creación de la carpeta RECYCLER

Tabla 5.14: Detalle regla impedir la creación de la carpeta RECYCLER

REGLA	REGLA INTERNA	PROCESO O RUTA SOBRE EL CUAL SE TOMA DESCISIÓN	ACCIÓN
Impedir la creación de la carpeta RECYCLER **Procesos:** * **Excepciones:** Ninguna	Bloqueo de creación de la carpeta RECYCLER	• ***\RECYCLER (enable drive types)	Bloquear Acceso de Modificación/ Creación/ Borrado

- **Bloquear el acceso al Autorun.inf:** La regla en mención bloquea el acceso al archivo autorun.inf alojado en los medios extraíbles, evitando de esta forma que cualquier aplicativo malicioso pueda acceder al fichero.

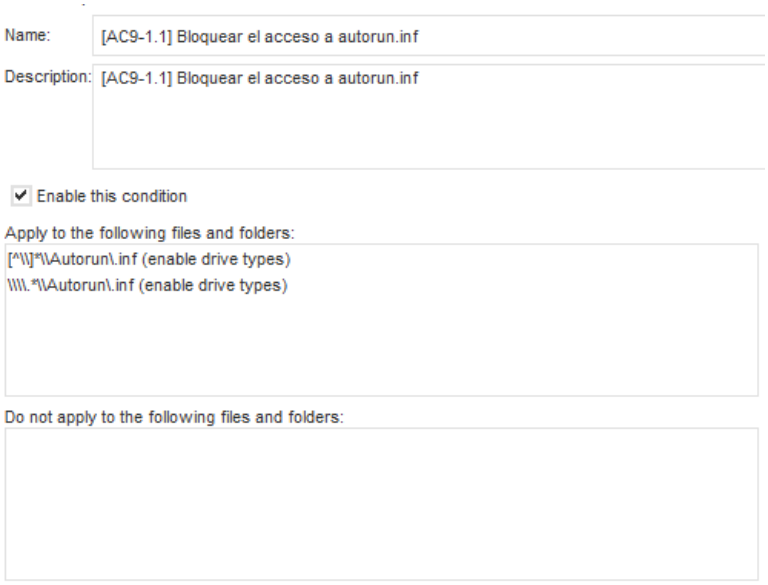


Figura 5.12: Bloquear el acceso al Autorun.inf

Tabla 5.15: Detalle regla bloquear el acceso al Autorun.inf

REGLA	REGLA INTERNA	PROCESO O RUTA SOBRE EL CUAL SE TOMA DESCISIÓN	ACCIÓN
Bloquear el acceso al Autorun.inf **Procesos:** %windir%\explorer.exe %windir%\System32\explorer.exe %windir%\SysWOW64\explorer.exe Excepciones: Ninguna	Autorun.inf	• [^\\]*\\Autorun\.inf (enable drive types) • \\\\.*\\Autorun\.inf (enable drive types)	Bloquear Acceso Ejecución

- **Proteger los archivos del cliente y claves de registro:** En esta directiva se tiene como objetivo proteger los recursos sensibles en las computadoras tanto a nivel de sistema operativo Windows como de antivirus Symantec. Entre los recursos que se protegen en la regla se consideran los servicios, acceso al registro, acceso a archivos y carpetas, drivers, archivos del sistema y procesos de SEP.

Figura 5.13: Proteger los archivos del cliente y claves de registro

Tabla 5.16: Configuraciones de reglas de Control de aplicaciones

REGLA	REGLA INTERNA	PROCESO O RUTA SOBRE EL CUAL SE TOMA DESCISIÓN	ACCIÓN
Protect client files and registry keys : Procesos:* Excepciones: %windir%\system 32\services.exe %windir%\system 32\msiexec.exe •%windir%\syswo w64\msiexec.exe •HKEY_LOCAL_MA CHINE\SOFTWARE \Symantec\Syman tec Endpoint Protection\Migrati on\TargetPath#*\ *.exe	Servicios de Windows y SEP	•HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\ccEv tMgr** •HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\ccSe tMgr** •HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\ccSe tMgr** •HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\Eras erUtilRebootDrv** •HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\Smc Service** •HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\Snac Np** •HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\SPB BCDrv**	Bloquear Acceso de Modificación/ Creación/ Borrado

REGLA	REGLA INTERNA	PROCESO O RUTA SOBRE EL CUAL SE TOMA DESCISIÓN	ACCIÓN
Protect client files and registry keys : Procesos:* Excepciones: %windir%\system32\services.exe %windir%\system32\msiexec.exe •%windir%\syswow64\msiexec.exe •HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\Migration\TargetPath#**.exe	Acceso a Archivos y carpetas	•HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_installpath# •#HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_install_path#** •HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection •#HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SysPlant\SysFer\SEPBaseDir#**	Bloquear Acceso de Modificación/ Creación/ Borrado
	Acceso a Drivers	system32\drivers\COH_Mon.sys system32\drivers\srtsp.sys system32\drivers\srtspl.sys system32\drivers\srtspx.sys system32\drivers\symdns.sys system32\drivers\SYMEVENT.SYS system32\drivers\symfw.sys system32\drivers\symids.sys	Bloquear Acceso de Modificación/ Creación/ Borrado
	Archivos del Sistema	system32\s32evnt1.dll system32\symneti.dll system32\symredir.dll system32\sysfer.dll system32\symvpn.dll	Bloquear Acceso de Modificación/ Creación/ Borrado
	Prevenir la terminación de los procesos de SEP	• ccApp.exe • ccSvcHst.exe • Rtvscan.exe • smc.exe • smcgui.exe • snac.exe • SymCorpUI.exe •#HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_install_path#*.exe • LiveUpdate\LU*.exe • LiveUpdate\lsetup.exe • Common Files\Symantec Shared*.exe •#HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SysPlant\SysFer\SEPBaseDir#**	Bloquear Acceso de Modificación/ Creación/ Borrado

5.4 CREACIÓN DE POLÍTICAS DE DISPOSITIVOS EN SEP

Las directivas de control de dispositivos nos permiten administrar de forma centralizada los dispositivos o medios extraíbles que están habilitados pasa su uso. Para ello SEP utiliza los GUID y el identificador de los dispositivos que tienen a nivel de hardware, debido a que los parámetros de identificación de los medios los asigna el fabricante.

En la captura mostrada a continuación, se utiliza la herramienta de Symantec DevViewer, el cual nos ayuda a obtener los identificadores físicos de los dispositivos.

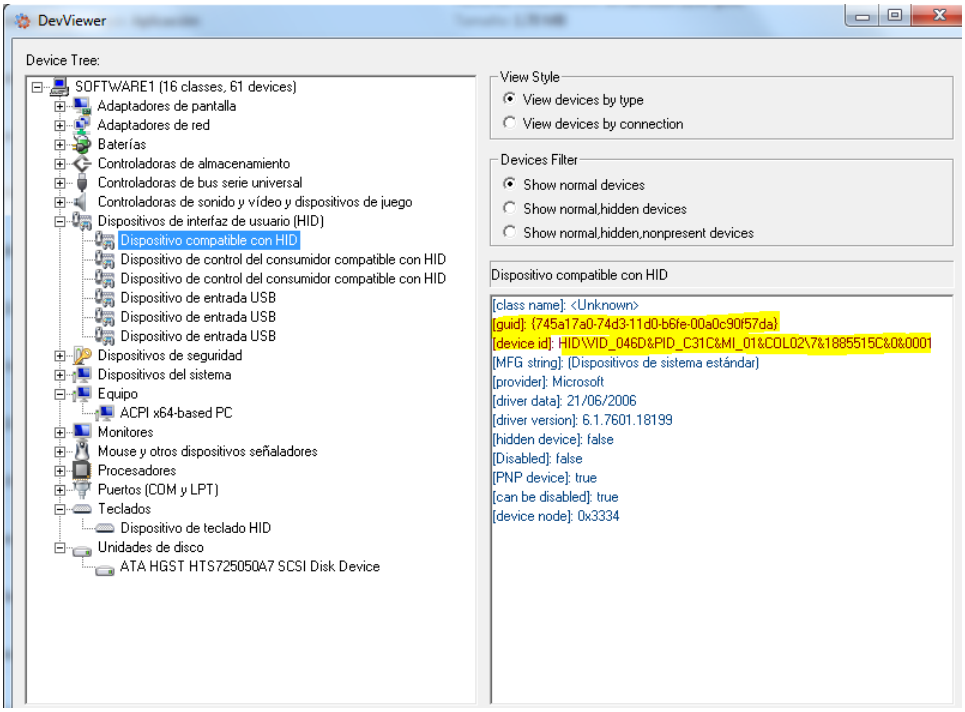


Figura 5.14: Visualización del ID del dispositivo

En la empresa existen usuarios que tienen habilitado el acceso a medios extraíbles y otros que tiene restringido el uso de USB, por lo cual para la implementación del

esquema se crearán las siguientes 2 directivas de control dispositivos, dependiendo sea el caso:

- Bloquear Medios Extraíbles Estaciones.
- Permitir Medios Extraíbles Estaciones.

Bloquear Medios Extraíbles Estaciones: Esta directiva tiene como objetivo bloquear medios extraíbles tales como USB, CD/DVD, medios de Bluetooth, entre otros. Cabe mencionar que a su vez la directiva permite el acceso a dispositivos de interface humana, impresoras, equipos USB utilizados para la atención al cliente (token, tarjetas de seguridad y contadores de dinero).

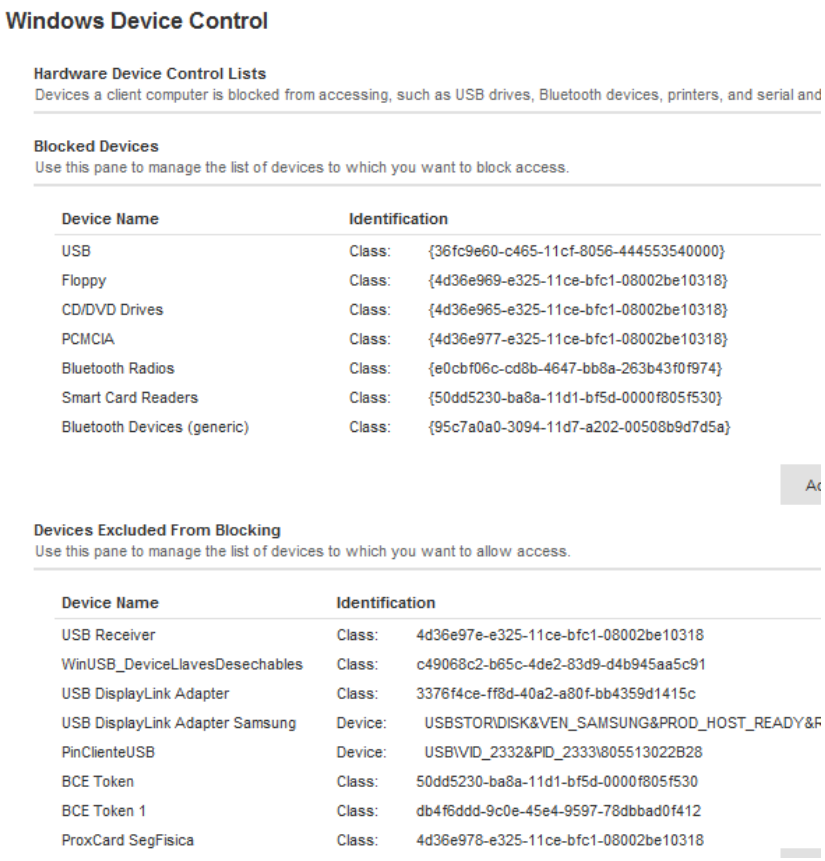


Figura 5.15: Control Dispositivos - Bloqueo Medios Extraíbles

A continuación se listan los dispositivos bloqueados y permitidos en la directiva.

Tabla 5.17: Dispositivos bloqueados por la directiva - Control de Apps

DISPOSITIVO	IDENTIFICADOR FISICO DEL DISPOSITIVO
USB	Class: {36fc9e60-c465-11cf-8056-444553540000}
Floppy	Class: {4d36e969-e325-11ce-bfc1-08002be10318}
CD/DVD Drives	Class: {4d36e965-e325-11ce-bfc1-08002be10318}
PCMCIA	Class: {4d36e977-e325-11ce-bfc1-08002be10318}
Bluetooth Radios	Class: {e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
Smart Card Readers	Class: {50dd5230-ba8a-11d1-bf5d-0000f805f530}
Bluetooth Devices (generic)	Class: {95c7a0a0-3094-11d7-a202-00508b9d7d5a}

Tabla 5.18: Dispositivos permitidos por la directiva - Control de Apps

DISPOSITIVO	IDENTIFICADOR FÍSICO DEL DISPOSITIVO
Human Interface Devices (Mice, Joysticks, Gamepads, and System controls)	Class: {745a17a0-74d3-11d0-b6fe-00a0c90f57da}
Printing Devices	Class: {4d36e979-e325-11ce-bfc1-08002be10318}
Controladoras de sonido y vídeo y dispositivos de juego	Class: {4d36e96c-e325-11ce-bfc1-08002be10318}
Network Adapters	Class: {4d36e972-e325-11ce-bfc1-08002be10318}
Infrared Devices	Class: {6bdd1fc5-810f-11d0-bec7-08002be2092f}
Imaging Devices (Scanners, Digital Cameras, etc)	Class: {6bdd1fc6-810f-11d0-bec7-08002be2092f}
Panini E172976	Device: USB\VID_121F&PID_0010\6&66CA680&1&5
Panini Ensobradora CH 01	Device: USB\VID_121F&PID_0001\6&CA680&1&1
Panini Ensobradora CH 02	Device: USB\VID_121F&PID_0002\6&66CA0&1&1
OLIVETTI	Device: USBPRINT\OLIVETTIIBM_PPII\8&216&0&USB001
USB Receiver	Class: 4d36e97e-e325-11ce-bfc1-08002be10318
WinUSB_LlavesDesechables	Class: c49068c2-b65c-4de2-83d9-d4b945aa5c91
USB DisplayLink Adapter	Class: 3376f4ce-ff8d-40a2-a80f-bb4359d1415c
USB DisplayLink Adapter Samsung	USBSTOR\DISK&VEN_SAMSUNG&PROD_HOST_READY&REV_1210\EGMS000000&0
PinClienteUSB	Device: USB\VID_2332&PID_2333\805513022B28
BCE Token	Class: 50dd5230-ba8a-11d1-bf5d-0000f805f530
BCE Token 1	Class: db4f6ddd-9c0e-45e4-9597-78dbbad0f412
ProxCard SegFisica	Class: 4d36e978-e325-11ce-bfc1-08002be10318

Permitir Medios Extraíbles Estaciones: Esta directiva es exclusivamente para habilitar el acceso a medios extraíbles y demás dispositivos a los altos ejecutivos de la empresa, por lo cual no se bloquean ningún instrumento.

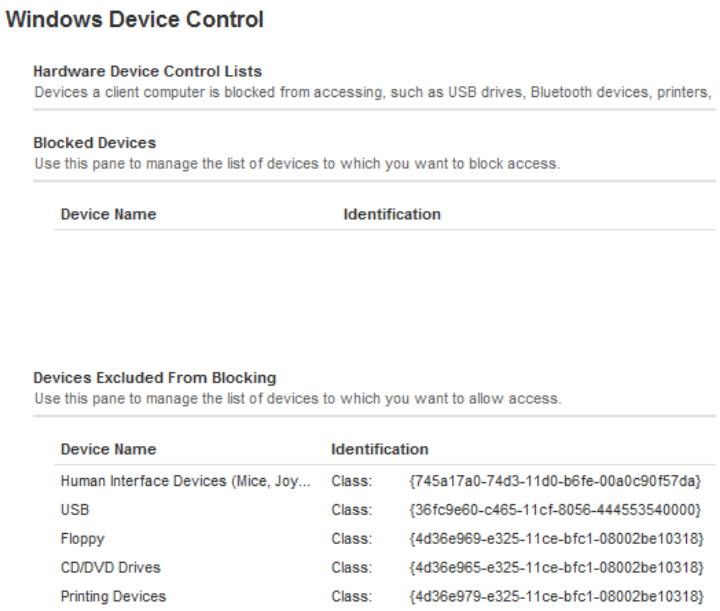


Figura 5.16: Control Dispositivos - Permitir Medios Extraíbles Equipos

Tabla 5.19: Dispositivos permitidos por directiva de Control de apps

DISPOSITIVO	IDENTIFICADOR FÍSICO DEL DISPOSITIVO
Human Interface Devices (Mice, Joysticks, Gamepads, and System controls)	Class: {745a17a0-74d3-11d0-b6fe-00a0c90f57da}
USB	Class: {36fc9e60-c465-11cf-8056-444553540000}
Floppy	Class: {4d36e969-e325-11ce-bfc1-08002b318}
CD/DVD Drives	Class: {4d36e965-e325-11ce-bfc1-0800210318}
Printing Devices	Class: {4d36e979-e325-11ce-bfc1-08002be318}
PCMCIA	Class: {4d36e977-e325-11ce-bfc1-08002be318}
Imaging Devices (Scanners, Digital Cameras, etc)	Class: {6bdd1fc6-810f-11d0-bec7-08002be2092f}
Bluetooth Radios	Class: {e0cbf06c-cd8b-4647-bb8a-26b43f0f974}
Smart Card Readers	Class: {50dd5230-ba8a-11d1-bf5d-0000f805f530}
Network Adapters	Class: {4d36e972-e325-11ce-bfc1-08002b318}
Storage Volumes	Class: {71a27cdd-812a-11d0-bec7-08002b92f}
Bluetooth Devices (generic)	Class: {95c7a0a0-3094-11d7-a202-00508d5a}

Al no tener un control sobre que dispositivos y que información guardan los usuarios en los medios, se ha creado una alerta en la consola de administración en la cual informe cuando un usuario a ingresado una memoria flash y que información accedido en la misma. En la siguiente imagen se muestra un ejemplo de una alerta generada por la directiva.

Notification Name	Type	Condition	Actions
Alerta Medios Extraibles PCs	Client security alert	1 within 1 minute	Email to [redacted]

Figura 5.17: Alerta Medios Extraíbles en PC's configurada en la SEPM

Asunto: I.SEP.AP.3.1-Accesos no autorizados desde PC con dispositivos USBNICAlert-Security.NIC Security Correlated Class::Low

Acceso exitosos o no exitosos con dispositivos USB en estaciones de trabajo.

View Name	Seguridad SEP
Date/Time	Jan 30 11:56:39
Event Category	System.Errors.Peripherals
Current Severity	Low (1/5)
Count	35
NIC Category	System
Alert Category	System.Errors
Message ID	FileWrite:03
Message Text	Jan 30 11:49:30 [redacted] SymantecServer:[redacted],Continue,[AC5-1.1] Registrar la escritura de archivos en unidades USB,Fil Registrar la escritura de archivos en unidades USB | [AC5-1.1] Registrar la escritura de archivos en unidades USB,2348,C:/Program Files Name,G:/REINGENIERIA ESTRELLA 1/Juicios y Afirmaciones/JUICIOS Y AFIRMACIONES R.pptx,User:[redacted],Domain:[redacted]Act USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_PMAP\001731F2A889B010899EAFE5&0
Correlation Message ID	I-SEP-AP-3-1
Correlation Message Text	Accesos no autorizados desde PCs con dispositivos USB

Figura 5.18: Notificación recibida por correo, por inserción de medios extraíbles

5.5 CREACIÓN DE POLÍTICAS DE FIREWALL EN SEP

Las directivas host firewall en SEP nos permiten administrar de forma centralizada las comunicaciones permitidas entre los equipos de la infraestructura. Para ello se realizó un levantamiento de información acerca de las comunicaciones que fluyen entre las estaciones y los aplicativos.

La primera actividad para la identificación de las comunicaciones válidas, ha sido poner en modo escucha (sin bloqueo) la regla de firewall por defecto en las estaciones, a fin de obtener en los respectivos registros de tráfico las conexiones de los programas cliente servidor.

Posterior al registro del tráfico, se ha validado con el área de Desarrollo, las comunicaciones de los aplicativos críticos y sensibles para la compañía, logrando tener en consideración los siguientes registros, los cuales se consideran reglas de acceso dentro de la directiva de firewall en estaciones:

Tabla 5.20: Comunicaciones Permitidas por directiva de Firewall

No.	Nombre de la regla	Aplicación	Grupo Origen	Grupo Destino	Servicio	Acción
1	Permitir Conexiones AD	Any	AD Server Redes Usuarios	AD Server Redes Usuarios	[TCP:[Puertos Autenticación], UDP:[123]]	**Permitir**
2	Neoteller - Ventanillas	[C:\Neoteller\config.exe]	Redes Usuarios	Servidor NeoTeller	[Puerto 8443, Puerto 9443, 443]	**Permitir**
3	Gestor Documental	C:\Program Files\Java\jre7\bin\javaw.exe, C:\Program Files (x86)\Java\jre7\bin\javaw.exe, C:\Program Files\WINPAKPRO\Winpak2.exe	Redes Usuarios	Servidor Neo Comercial, Servidor Gestor Documental	Puertos NeoComercial, Puerto 8080	**Permitir**

No.	Nombre de la regla	Aplicación	Grupo Origen	Grupo Destino	Servicio	Acción
4	Syscards Debit	[c:\Program Files\Tech Soft\Syscard Debit\sdebit.exe]	Redes Usuarios	Servidores Tarjetas Crédito	[Puertos Syscards, Puerto 8704]	**Permitir**
5	Acceso Onbase	[C:\Program Files\Onbase Client*]	Redes Usuarios	Servidores OnBase	[HTTP Ports, Puerto 1433, Puerto 9443]	**Permitir**
6	Acceso Portal CRM	[]	Redes Usuarios	Servidores CRM	[Puertos CRM, Puerto 80]	**Permitir**
7	Altitude uAgent	C:\Program Files (x86)\Altitude\Altitude uCI 7.5\Altitude uAgent Windows\uagentwindows.exe,	Redes Usuarios	Altitude uAgent	[Puertos Altitud uAgent, Puerto 7443]	**Permitir**
8	Extreme SNA 2016 & Pantallas	[*]	Redes Usuarios	Servidores HIS, Servidores CORE	[Puertos ExtremeSNA, Puerto 5443]	**Permitir**

POLÍTICA DE FIREWALL – SEP 14 ESTACIONES

La directiva de firewall de estaciones se ha definido a nivel de la consola de administración de clientes de SEP, la misma que contiene todas las comunicaciones permitidas de los aplicativos.

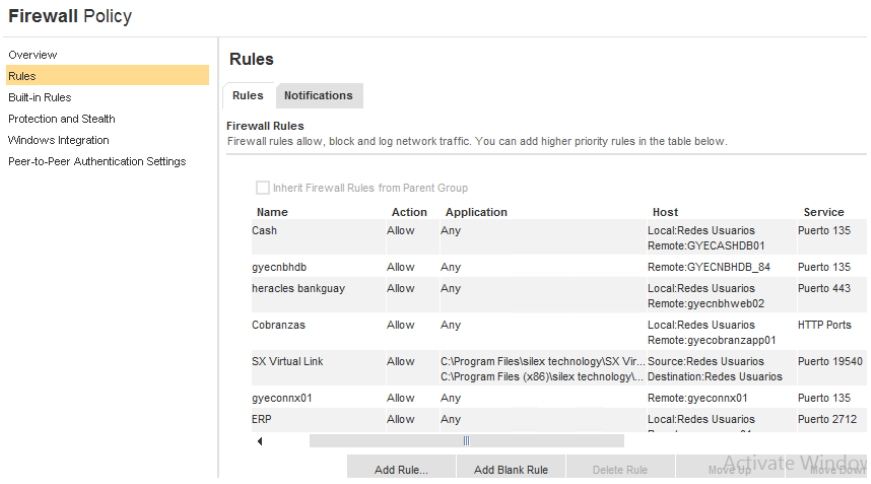


Figura 5.19: Política de Firewall en Estaciones

La directiva de firewall se tiene dos reglas de bloqueo, cuya comunicación no está permitida desde las estaciones y las cuales se encuentran al final de la lista de acceso.

Bloqueo Carpetas Compartidas: Esta regla tiene como objetivo bloquear las carpetas compartidas es las estaciones de los usuarios, las cuales en muchas ocasiones son utilizadas por los programas maliciosos para comprometer e infectar otros ordenadores.

Tabla 5.21: Regla Bloqueo de Carpetas Compartidas

No.	Nombre de la regla	Aplicación	Grupo Origen	Grupo Destino	Servicio	Acción
50	Bloquear Carpetas Compartidas	Any	Redes Usuarios	Redes Usuarios, Redes Servidores	[Puerto 445]	Block

Bloqueo Comunicaciones No Permitidas: Esta regla tiene como objetivo bloquear todas las conexiones no identificadas en el levantamiento de información, las mismas que no están permitidas. En caso de que se requiera permitir una nueva conexión se deberá crear una regla puntual para permitir la comunicación deseada.

Tabla 5.22: Regla Bloqueo Comunicaciones No Permitidas

No.	Nombre de la regla	Aplicación	Grupo Origen	Grupo Destino	Servicio	Acción
51	Bloquear Comunicaciones No Permitidas	Any	Any	Any	Any	Block

De acuerdo con el levantamiento de información realizado previamente, se lograron identificar 49 reglas de conexión las cuales forman parte en la directiva de firewall creada. A continuación se detallan las reglas restantes que forman parte de la directiva generada:

Tabla 5.23: Reglas definidas en la directiva Firewall local

No.	Nombre de la regla	Aplicación	Grupo Origen	Grupo Destino	Servicio	Acción
9	Permisos de RDP a Estaciones & Servidores	C:\Windows \System32\ msra.exe, C:\Windows \System32\ mstsc.exe]	Redes Usuarios	Redes Usuarios, Redes Servidores	[Puerto 3389, Puerto 135, Puerto 8443]	Allow
10	Transferencia Panini Ventanilla Extensiones	[C:\Program Files\Cheqsc an\PMSCAN. exe]	Redes Usuarios	Estaciones JefeOperati vo	[Puerto 1433]	Allow
12	Permitir Rutas de Windows	[C:\Program Files\Micros oft Policy Platform\pol icyHost.exe, C:\Windows \System32\ wbem\WmiP rvSE.exe	Redes Usuarios	Redes Servidores	[HTTP Ports, Puerto 139, Puerto 445, Puerto Rutas Windows]	Allow
12	Cash	[]	Redes Usuarios	CASH DB	[Puerto 135]	Allow
13	Administración Web Banqueros Mi Barrio	[]	Redes Usuarios	Servidores Banqueros	[Puerto 443]	Allow
14	Acceso Cobranzas y Deudas	[]	Redes Usuarios	Servidor Cobranzas	[HTTP Ports]	Allow
15	SX Virtual Link	C:\Program Files (x86)\silex technology\S Virtual\Conn ect.exe	Redes Usuarios	Redes Usuarios	[Puerto 19540]	Allow
16	Sistema ERP - Dynamics	[]	Redes Usuarios	Servidor ERP Dynamics	[Puerto 2712]	Allow
17	Acceso a Owa Correo Electrónico	[]	Redes Usuarios	Servidores Internos Correo	[Puerto 443]	Allow
18	Autodiscover Correo Electrónico - Outlook	C:\Program Files\Micros oft Office*	Redes Usuarios	Servidor Hibrido Correo - Exchange Online, Servidores Hibrido Lync - Skype Empresarial	[HTTP Ports, Puerto 8080, Puerto 5061]	Allow

No.	Nombre de la regla	Aplicación	Grupo Origen	Grupo Destino	Servicio	Acción
19	Comunicación Antivirus Symantec	[]	Redes Usuarios	Servidor Symantec, Servidor LiveUpdate Admin	[Puerto 9443, Puerto 7070]	Allow
20	FileServer	[]	Redes Usuarios	FileServer01 FileServer02 FileServer03	[Puerto 445]	Allow
21	Acceso a Históricos	[]		Servidor HistoricoDB	1433,445	Allow
22	Administrador de Servicios	[]	Redes Usuarios	Servidro HP Web	[Puerto 8080]	Allow
23	Acceso Wireless	[]	Redes Usuarios	Servidor Acceso Wireless	[Puertos IMC]	Allow
24	Acceso Inteligencia de Negocio	[]	Redes Usuarios	Servidor IntNeg	[Puerto 4433]	Allow
25	Intranet del Corporativo	[]	Redes Usuarios	intranet.banco.com	[]	Allow
26	Acceso Internet - Servidor Proxy	C:\Program Files\Microsoft Office*	Redes Usuarios	Servidor Proxy	[Puerto 8080]	Allow
27	Reportes Bancarios	[]	Redes Usuarios	Servidor de Reportes	[HTTP Ports]	Allow
28	Licenciamiento KMS Office	[]	Redes Usuarios	Servidor Licencias	[Puerto 1699]	Allow
29	Monitor Transaccional	[]	Redes Usuarios	Servidores MonitorPlus	[Puerto 135, Puerto 1433, Puerto 445]	Allow
30	DHCP	[]	Redes Usuarios	Servidores DHCP	Puertos DHCP	Allow
31	Generación Documentos - Pólizas	[]	Redes Usuarios	Equitrac01, Equitrac02,	[Puerto 445, Puerto 135, Puerto 2910]	Allow
32	Servicio de Impresión	[]	Redes Usuarios	PRINT SERVER01	[Puerto 445, 7370]	Allow
33	Acceso Transacciones Core	c:\ProgramData\Microsoft\Windows\Start Menu\Programs\SX Virtual Link\Connect.exe]	Redes Usuarios	Sevidores Microfocus	[Puerto 135, Puerto 43250]	Allow

No.	Nombre de la regla	Aplicación	Grupo Origen	Grupo Destino	Servicio	Acción
34	Servidor RMS	[]	Redes Usuarios	Servidor RMS Local	[HTTP Ports]	Allow
35	Acceso Aplicativo Recursos Humanos	[]	Redes Usuarios	Serviores RRHH	[HTTP Ports]	Allow
36	Despliegues SCCM	[]	Redes Usuarios	Servidores SCCM	[Puertos SCCM]	Allow
37	Aplicativo Cumplimiento y Riesgo	[]	Redes Usuarios	Servidores Cumplimien to	[HTTP Ports]	Allow
38	Gestionador de Tickets	[]	Redes Usuarios	Servidor SIGD	[Puerto 443]	Allow
39	Cursos Formación Virtual	[]	Redes Usuarios	Servidor Web Campus	[HTTP Ports]	Allow
40	Administración WorkLoad	[]	Redes Usuarios	Servidor WLoad01	[Puerto 7598]	Allow
41	Acceso Sitios Externos del Corporativo	[]	Redes Usuarios	Sitios Externos	[HTTP Ports]	Allow
42	Sitio Web Principal	[]	Redes Usuarios	Servidores Web Sitio Corporativo	[Puerto 443]	Allow
43	Acceso CardHolder	[]	Redes Usuarios	Servidores CardHolder	[Puerto 8443]	Allow
44	Administración Extreme ATMs	[C:\kt2143\K TQMA.exe]	Redes Usuarios	Servidores Extreme ATMs	[Puerto 135, 9345]	Allow
45	Servidores Aplicativos Web	[]	Redes Usuarios	APPWEBxx	[HTTP Ports]	Allow
46	Acceso Aplicativos Web	[]	Redes Usuarios	appweb	Puertos FIRMAS	Allow
47	Nexus OfficeApps	[]	Redes Usuarios	nexus officeapps live	[Puerto 443]	Allow
48	Acceso Servicio de Federación Office 365	C:\Program Files\Interne t Explorer\iex plore.exe	Redes Usuarios	Sitio STS, Sitio Sharepoint, Sitio Onedrive	[Puerto 443, Puerto 80]	Allow
49	Servidores Alarmas - Seguridad Física	C:\RASplus\R ASplus_Runn er.exe	Redes Usuarios	Servidores Alarmas	Puerto 137, 138, 1433, 7854	Allow
50	Bloquear Carpetas Compartidas	Any	Redes Usuarios	Redes Usuarios, Redes Servidores	Puerto 445	Block
51	Bloquear Comunicaciones No Permitidas	Any	Any	Any	Any	Block

5.6 CREACIÓN DE POLÍTICAS DE PREVENCIÓN DE INTRUSOS EN SEP

Las directivas de prevención de intrusos, protegen a los ordenadores de método específicos que pueden ser aprovechados por programas maliciosos para acceder a la red. Adicionalmente las reglas de IPS analizan el tráfico de la red y su comportamiento, con el objetivo detectar y bloquear cualquier amenaza que aproveche un vector de ataque o vulnerabilidad en las estaciones.

POLÍTICA DE PREVENCIÓN DE INTRUSOS – SEP 14 ESTACIONES

Las directivas de protección de intrusiones de SEP contiene hasta momento 2665 vulnerabilidades identificadas y cuyas remediaciones se incluyen en sus definiciones de IPS. La directiva implementada tiene 206 firmas habilitadas a fin de que bloqueen las vulnerabilidades de acuerdo a su criticidad.

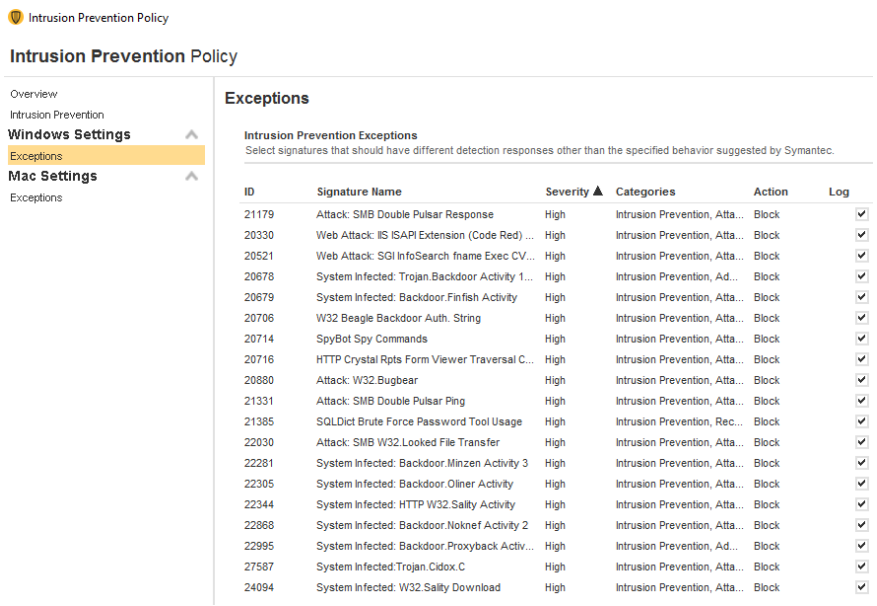


Figura 5.20: Política de Prevención de Intrusos para estaciones

Cabe indicar que no se ha activado en modo de bloqueo más firmas, debido a que las 2459 firmas restantes no se aplican a la plataforma.

Tabla 5.24: Distribución de Firmas de IPS configuradas

Tipo Acción - Firma IPS	Cantidad
Permitida	**2.459**
Bloqueada	**206**
Alta	191
Media	12
Baja	3
Total general	**2.665**

Entre las firmas más relevantes de IPS configuradas en la directiva, se encuentran las definiciones que bloquean la explotación de la vulnerabilidad “Microsoft SMB MS17-010 Disclosure Attempt”, la cual fue explotada por el malware “Ransom.Wannacry” a mediados del año 2017. [14]

Tabla 5.25: Firmas de IPS – Vulnerabilidad MS17-010

ID	NOMBRE FIRMA-VULNERABILIDAD	SEVERIDAD	CATEGORÍA	ACCIÓN
22534	System Infected: Malicious Payload Activity 9	Alta	Intrusion Prevention, Attack	Bloqueada
21179	Attack: SMB Double Pulsar Response	Alta	Intrusion Prevention, Attack	Bloqueada
23875	OS Attack: Microsoft SMB MS17-010 Disclosure Attempt	Alta	Intrusion Prevention, Attack	Bloqueada
23862	OS Attack: MS SMB Remote Code Execution CVE-2017-0144	Alta	Intrusion Prevention, Attack	Bloqueada

En el siguiente listado se detallan las categorías vulnerabilidades que actualmente se está protegiendo con las firmas de IPS habilitadas en modo de bloqueo.

Tabla 5.26: Categorías de Firmas de IPS configuradas

CATEGORÍA	SEVERIDAD
Intrusion Prevention, Attack, Malcode, Trojan	Alta
Intrusion Prevention, Adware, Potentially Unwanted Application (PUA), Security Risk	Alta
Intrusion Prevention, Attack, Malcode	Alta
Intrusion Prevention, Attack, Backdoor, Malcode	Alta
Intrusion Prevention, Attack, Backdoor, Bot, DDOS, DOS, Malcode, Worm	Alta
Intrusion Prevention, Attack, Backdoor, Malcode, Worm	Alta
Intrusion Prevention, Reconnaissance, Scanner	Alta
Intrusion Prevention, Attack, Malcode, Worm	Alta
Intrusion Prevention, Attack, Backdoor, Malcode, Trojan	Alta
Intrusion Prevention, Security Risk	Alta
Intrusion Prevention, Attack, DOS	Alta
Intrusion Prevention, Attack, Backdoor	Alta
Intrusion Prevention, Attack, Bot, Malcode	Alta
Intrusion Prevention, Audit	Baja
Intrusion Prevention, Attack, Buffer Overflow	Media
Intrusion Prevention, Attack	Media
Intrusion Prevention, Probe, Reconnaissance	Media
Intrusion Prevention, Protocol Anomaly, Suspicious Event	Media

5.7 CREACIÓN DE POLÍTICAS DE INTEGRIDAD DE EQUIPO EN SEP

Las directivas de integridad de host de SEP ayudan en el aseguramiento de los equipos, mediante el cumplimiento de las políticas de seguridad definidas por la empresa. Dichas políticas nos ayudan a verificar si las estaciones cuentan con prerrequisitos tales como parches instados, valores en claves de registro, programas instalados, entre otros.

POLÍTICA DE INTEGRIDAD DE EQUIPO – SEP 14 ESTACIONES

La directiva de integridad de equipo implementada, ha sido creada con la finalidad de verificar si las estaciones cumplen con los siguientes 2 requisitos:

- Verificación de actualizaciones críticas a nivel de sistema operativo.
- Depuración de Administradores locales no permitidos.

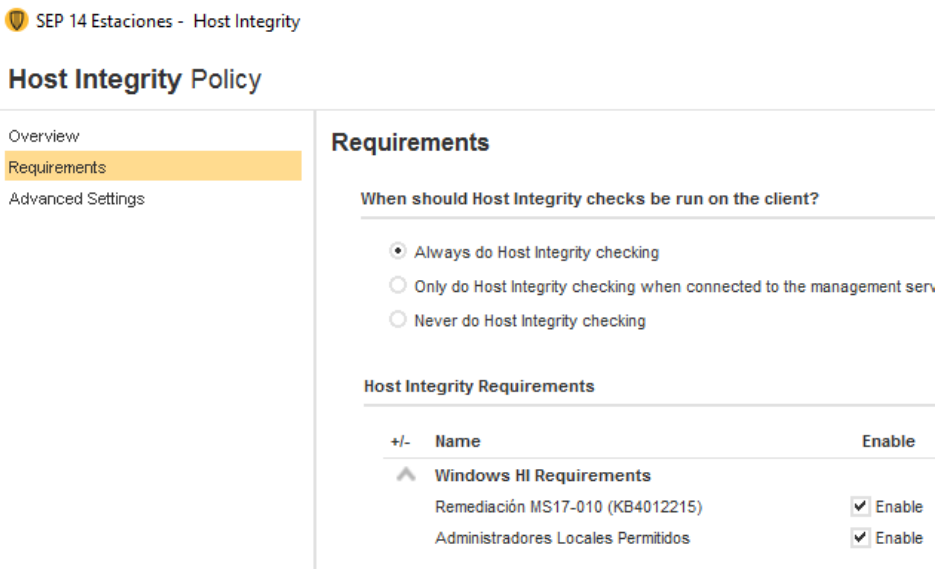


Figura 5.21: Política de Integridad de Estaciones

Verificación de actualizaciones críticas a nivel de sistema operativo: El objetivo principal de esta regla es verificar alguna actualización puntual con la que debe contar el sistema operativo del equipo. En la directiva se verifica si las estaciones cuentan con el parche KB4012215, el cual remedia la vulnerabilidad “Microsoft SMB MS17-010 Disclosure Attempt”.

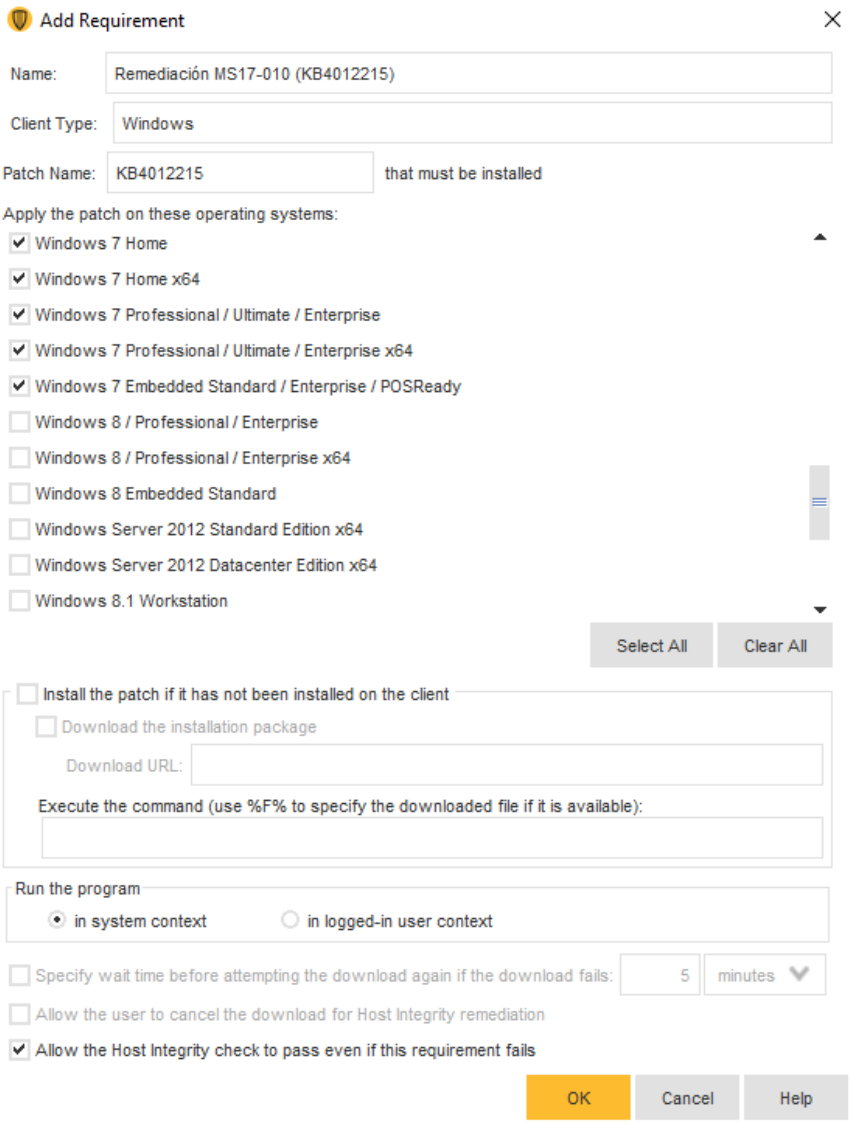


Figura 5.22: Verificación de actualizaciones críticas a nivel de S.O

Depuración de Administradores locales no permitidos: Esta regla nos ayuda a depurar y mantener únicamente los administradores locales permitidos en las estaciones. Para lograr esta funcionalidad se ha seleccionado la ejecución personalizada en regla, la cual nos permite ejecutar un script vbs.

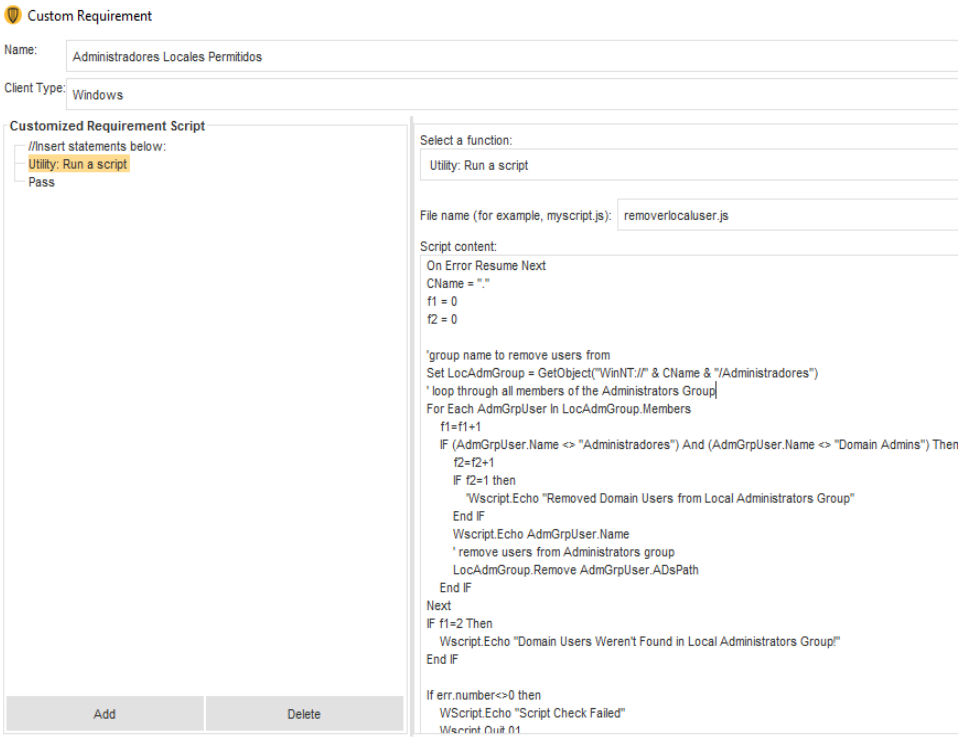


Figura 5.23: Integridad Equipo Depuración Administradores Locales No Permitidos

5.8 PRUEBAS Y MANTENIMIENTOS DE POLÍTICAS RESTRICTIVAS POSTERIOR A LA SALIDA A PRODUCCIÓN

Esta sección tiene como objetivo detallar los cambios, ajustes o mantenimientos que se han realizado a las políticas creadas en el esquema debido a su restrictividad.

POLÍTICA DE CONTROL DE ANTIVIRUS – SEP 14 ESTACIONES

La directiva de control de antivirus no ha sido necesario de ajustar o corregir, debido a que la misma está basada en las mejores prácticas indicadas por Symantec. Adicionalmente el nivel de análisis de la reputación de los posibles archivos maliciosos tiene una configuración intermedia, a fin de evitar los posibles falsos positivos generados.

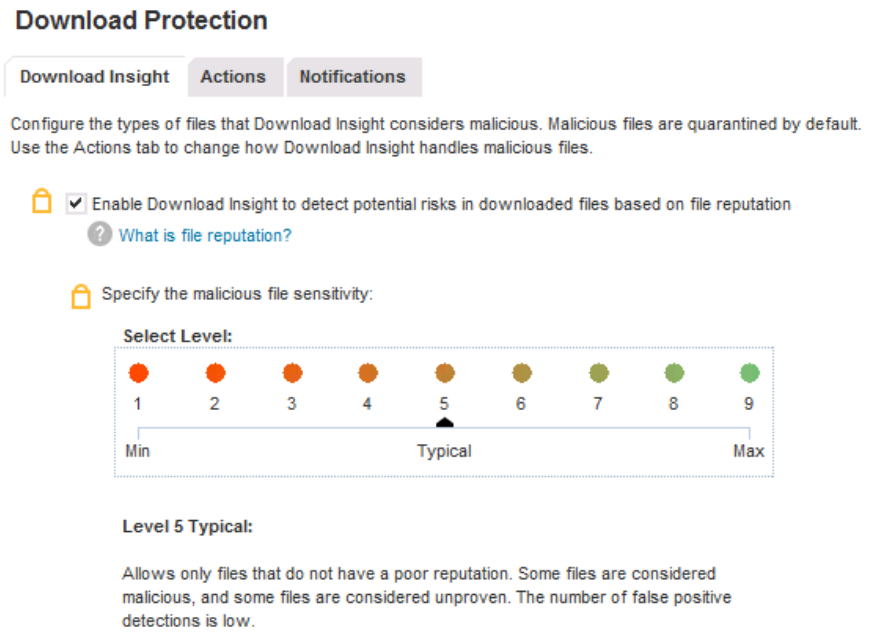


Figura 5.24: Nivel de configuración de Download Protection

POLÍTICA DE CONTROL DE APLICACIONES – SEP 14 ESTACIONES

La política de control de aplicaciones, constantemente está siendo actualizada debido a que posee 2 reglas en la cual se permite o bloquea algún tipo de recurso. A continuación se detallan los cambios realizados en cada regla:

- **Bloquear la ejecución de aplicaciones no permitidas:** Posterior a la creación de la regla, se han agregado las siguientes rutas de programas que no fueron identificados en el levantamiento de información y que fueron agregadas en las fases de piloto.

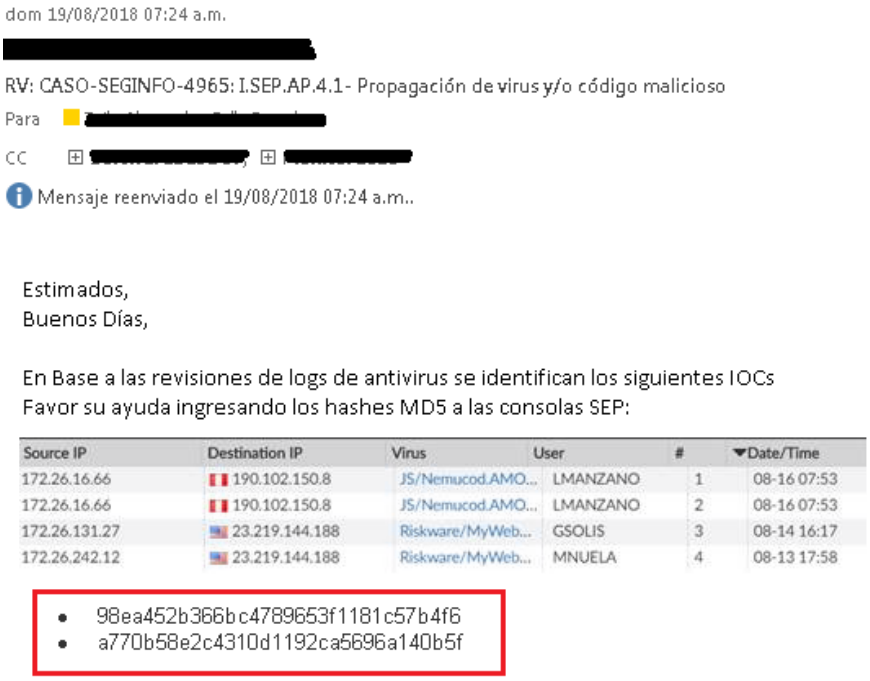
Tabla 5.27: Aplicaciones Identificadas en el Piloto Agencias

Ruta Agregada	Comentarios	Área
C:\Program Files\Foxit Software\Foxit Reader**	PDF	Banca Personal
C:\Program Files (x86)\Foxit Software\Foxit Reader**	PDF	Banca Personal
C:\Program Files\TextPad 7**	Editor Texto	Banca Personal
C:\Program Files (x86)\TextPad 7**	Editor Texto	Banca Personal
C:\Users\%username%\AppData\Local\Microsoft**	Ejecutables utilizados por IE	Banca Corporativa
C:\Users\%username%\AppData\Local\Apps\2.0**	Reporteador Hyland	FO Validación
C:\Program Files\Microsoft Dynamics AX**	Aplicativo – ERP	FO Validación
C:\Program Files (x86)\Microsoft Dynamics AX**	Aplicativo – ERP	FO Validación
C:\Program Files\Microsoft Dynamics AX 2012 Data Import Export Framework Client Component**	Aplicativo – ERP	FO Validación
C:\Program Files (x86)\Microsoft Dynamics AX 2012 Data Import Export Framework Client Component**	Aplicativo – ERP	FO Validación
\\gyeofacapp01\Bridger**	Aplicativo - BridgerInsight	Cumplimiento
C:\Program Files\Notepad++**	Editor Texto	Cumplimiento
C:\Program Files (x86)\Notepad++**	Editor Texto	Cumplimiento
C:\Program Files\TextPad 4**	Editor Texto	Cumplimiento
C:\Program Files (x86)\TextPad 4**	Editor Texto	Cumplimiento
C:\Program Files\debug**	Aplicativo - Admin Regla Negocio	Cumplimiento

Tabla 5.28: Aplicaciones Identificadas en el Piloto Matriz

Ruta Agregada	Comentarios	Área
C:\TS\run**	Aplicativo - Turbo Switf	Cumplimiento
C:\Program Files\TextPad 8**	Editor Texto	Auditoria
C:\Program Files\RSA SecurID Software Token**	Genera Token para acceder al site MasterCard	Banca Personal
C:\Windows\splwow64.exe	Utilizado para imprimir desde IE	Auditoria
C:\Windows\explorer.exe	Utilizado por CheqScan	Jefe Operativo
C:\Program Files\Sargent & Greenleaf, Inc\Lock Management System** C:\ Program Files (x86)\Sargent & Greenleaf, Inc\Lock Management System**	LMS(Claves Desechables ATMs)	OPERACIONES SUCURSALES Y AGENCIAS
C:\Compartir\Cliente**	Monitoreo ATMs	OPERACIONES SUCURSALES Y AGENCIAS
C:\Cumplimiento\FATCA\IDES**	Utilitario Fatca	Cumplimiento
C:\aplicacion cupos*\	Procesos Evolution	Talento Humano
C:\KT2143**	Turnero KTQMA	SUCURSALES Y AGENCIAS
\\gyemplusapp01\MONITOR**	Aplicativo - Monitor Plus(EXE en server)	Prevención y Fraudes
C:\Cumplimiento\2017\Comite**	Conexión del proyector del directorio	Cumplimiento
C:\Program Files (x86)\IBM\Client Access** C:\Program Files\IBM\Client Access** C:\Program Files (x86)\CheckPoint\EndPoint Connect**	Conexión y revisión de informes médicos IESS	Dispensario Médico
C:\Program Files\ECI-BCE** C:\Program Files (x86)\ECI-BCE**	Firmar electrónicament e los DOCs BCE	FABRICA DE OPERACIONES
C:\Program Files\PrintingWindowsService** C:\Program Files (x86)\PrintingWindowsService**	Servicio Impresión - Cartas de Referencia	FABRICA DE OPERACIONES
ec96fc02a0cbd8a196b4cb599ac4e42a	Ejecutable Infocus Wireless - Proyector Wireless	METODOS

- **Bloquear por hash la ejecución de archivos maliciosos reportados:** Debido a los últimos ataques dirigidos reportados a las diferentes entidades bancarias latinoamericanas, se tienen constantes requerimientos por parte del área de seguridad de la información en referente al bloqueo archivos maliciosos en base a su hash. Hasta el momento se han agregado 482 hash MD5 y SHA256 los cuales correspondes a los diferentes boletines de seguridad.


dom 19/08/2018 07:24 a.m.

[redacted]

RV: CASO-SEGINFO-4965: I.SEP.AP.4.1- Propagación de virus y/o código malicioso

Para [redacted]

CC [redacted]

Mensaje reenviado el 19/08/2018 07:24 a.m..

Estimados,
Buenos Días,

En Base a las revisiones de logs de antivirus se identifican los siguientes IOCs
Favor su ayuda ingresando los hashes MD5 a las consolas SEP:

Source IP	Destination IP	Virus	User	#	Date/Time
172.26.16.66	190.102.150.8	JS/Nemucod.AMO...	LMANZANO	1	08-16 07:53
172.26.16.66	190.102.150.8	JS/Nemucod.AMO...	LMANZANO	2	08-16 07:53
172.26.131.27	23.219.144.188	Riskware/MyWeb...	GSOLIS	3	08-14 16:17
172.26.242.12	23.219.144.188	Riskware/MyWeb...	MNUELA	4	08-13 17:58

- 98ea452b366bc4789653f1181c57b4f6
- a770b58e2c4310d1192ca5696a140b5f

Figura 5.25: Ejemplo de requerimiento de bloqueo hash archivo malicioso

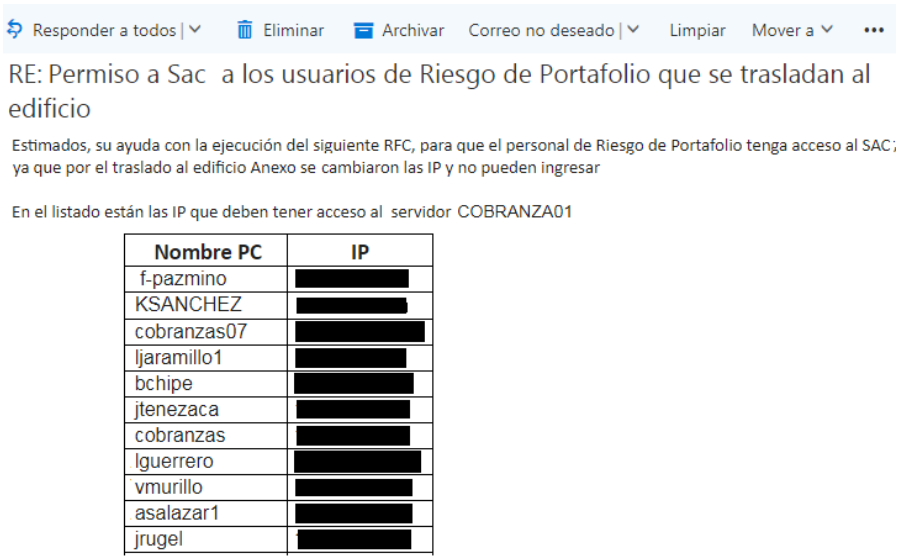
POLÍTICA DE CONTROL DE DISPOSITIVOS – SEP 14 ESTACIONES

La directiva de control de aplicaciones desde su puesta en producción, ha sido modificada una sola vez, debido a que uno dispositivos de seguridad con interfaz USB estaba siendo bloqueado por la directiva.

Figura 5.26: Ejemplo Requerimiento Habilitación ID de Dispositivo

POLÍTICA DE FIREWALL – SEP 14 ESTACIONES

La directiva de firewall en estaciones es una de las directivas en las que más mantenimientos o actualizaciones se realizan, debido a que constantemente se ejecutan requerimientos por proyectos o accesos a usuarios finales. En la siguiente captura se puede observar el tipo de solicitud que se realiza para proceder con la actualización de la política.



Responder a todos | Eliminar Archivar Correo no deseado | Limpiar Mover a •••

RE: Permiso a Sac a los usuarios de Riesgo de Portafolio que se trasladan al edificio

Estimados, su ayuda con la ejecución del siguiente RFC, para que el personal de Riesgo de Portafolio tenga acceso al SAC; ya que por el traslado al edificio Anexo se cambiaron las IP y no pueden ingresar

En el listado están las IP que deben tener acceso al servidor COBRANZA01

Nombre PC	IP
f-pazmino	[redacted]
KSANCHEZ	[redacted]
cobranzas07	[redacted]
ljaramillo1	[redacted]
bchipe	[redacted]
jtenezaca	[redacted]
cobranzas	[redacted]
lguerrero	[redacted]
vmurillo	[redacted]
asalazar1	[redacted]
jrugel	[redacted]

Figura 5.27: Ejemplo Requerimiento Habilitación Comunicación hacia Servidor

POLÍTICA DE INTEGRIDAD DE EQUIPO – SEP 14 ESTACIONES

En la directiva cumplimiento de integridad de equipos no ha sufrido algún tipo de modificación, debido a que la misma cumple con funciones específicas de validación y ejecución, tareas que han sido implementadas en base a requerimientos de las respectivas áreas de control.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 ANÁLISIS DE RESULTADOS OBTENIDOS CON LA APLICACIÓN DE POLÍTICAS RESTRICTIVAS

RESULTADOS POLÍTICA DE CONTROL DE ANTIVIRUS EN ESTACIONES

La directiva de análisis de virus implementada ha tenido una mayor detección de archivos maliciosos, en comparación con la política permisiva por defecto que se encontraba configurada inicialmente.

Se han listado todas las detecciones en las estaciones de los 6 primeros meses posteriores a la implementación de la directiva, en contraste con las detecciones de la política por defecto en los últimos 6 meses, con el cual se tienen los siguientes resultados:

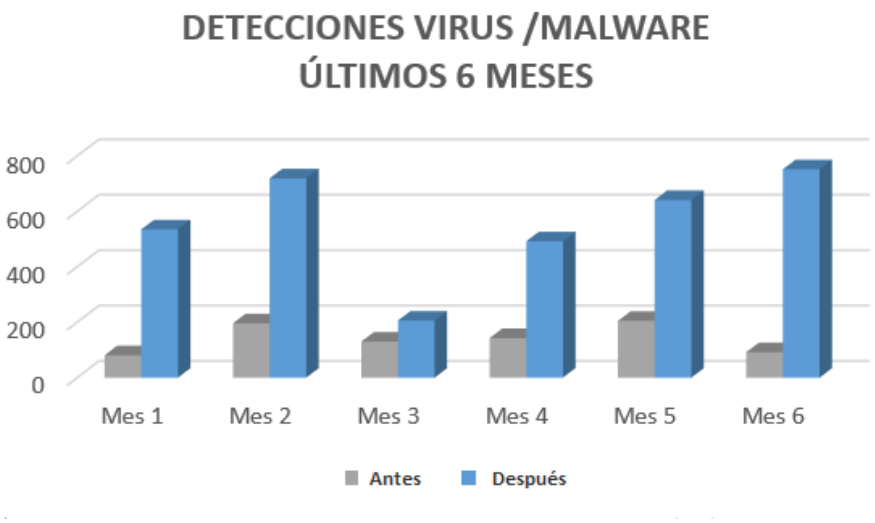


Figura 6.1: Detecciones de Virus y Malware en los últimos meses

Como se puede notar la cantidad de detecciones se ha incrementado en cada mes, posterior a su implementación de la directiva de control de antivirus en estaciones.

Tabla 6.1: Detecciones Virus/Malware en los últimos 6 meses

Mes	Antes	Después
Mes 1	81	535
Mes 2	196	719
Mes 3	130	206
Mes 4	143	492
Mes 5	205	641
Mes 6	92	752
TOTAL	**847**	**3.345**

El siguiente gráfico se puede observar el listado de los diferentes riesgos encontrados en las estaciones en los 6 meses posterior a implementación de la directiva.

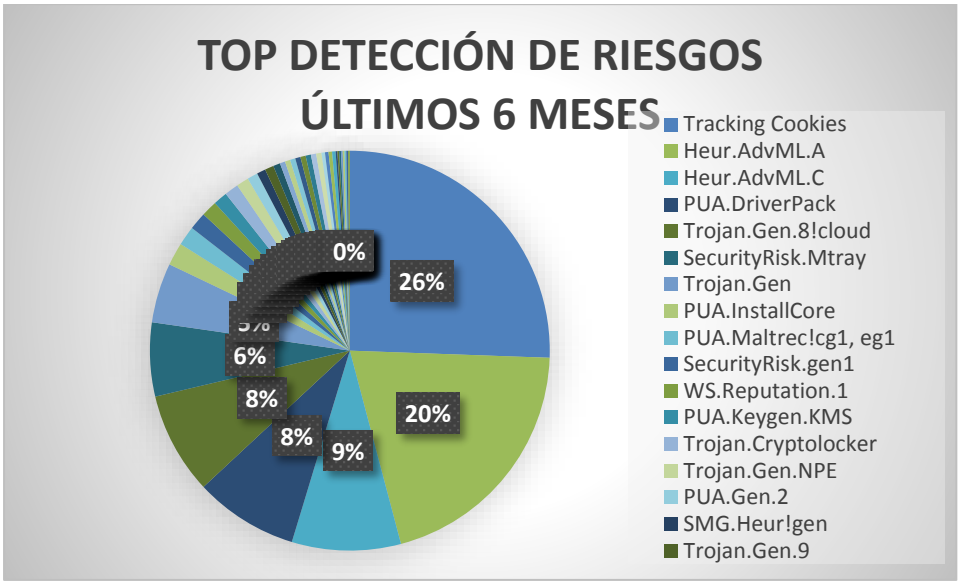


Figura 6.2: Top de Detecciones de Riesgo en los últimos 6 meses

RESULTADOS POLÍTICA DE CONTROL DE APLICACIONES ESTACIONES

Mediante la directiva de control de aplicaciones se ha bloqueado el acceso a aplicaciones nos permitidas que se encontraban instaladas en las estaciones de los usuarios.

En el siguiente gráfico se muestran los ejecutables en los cuales se ha intentado acceder en los tres últimos meses y cuya acción fue bloqueada por la directiva.

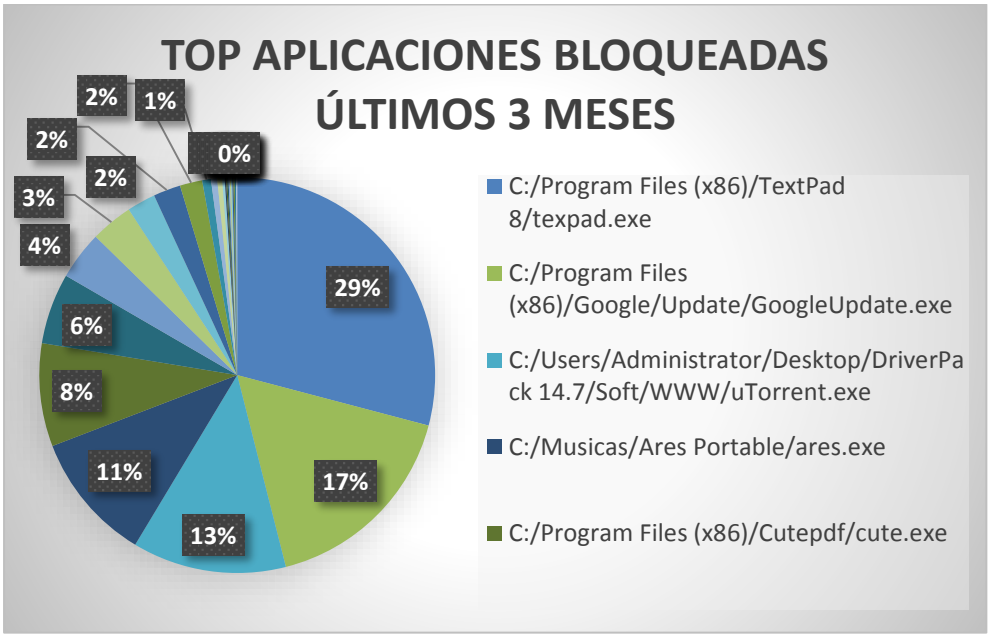


Figura 6.3: Top de aplicaciones bloqueadas en los últimos 3 meses

En los últimos 3 meses se ha identificado que se ha intentado acceder a los siguientes ejecutables 986 veces, de acuerdo a la siguiente tabla:

Tabla 6.2: Listado ejecutables bloqueados con mayores intentos en últimos 3 meses

APLICACIÓN BLOQUEADA	INTENTOS ACCESO
C:/Program Files (x86)/TextPad 8/texpad.exe	287
C:/Program Files (x86)/Google/Update/GoogleUpdate.exe	167
C:/Users/Administrator/Desktop/DriverPack 14.7/Soft/WWW/uTorrent.exe	124
C:/Musicas/Ares Portable/ares.exe	104
C:/Program Files (x86)/Cutepdf/cute.exe	83
C:/Reaspaldo/FIFA 10/emulador.exe	57
C:/Program Files (x86)/Common Files/Microsoft shared/OFFICE15/MSOSQM.EXE	39
C:/Program Files (x86)/TeamViewer/teamviewer.exe	34
C:/Program Files/Ask.com/UpdateTask.exe	23
C:/Program Files/Google/Update/GoogleUpdate.exe	22
C:/jveliz1/AppData/Local/GoToMeeting/g2mupdate.exe	18
Total general	**958**

Tabla 6.3: Listado ejecutables bloqueados con menores intentos en últimos 3 meses

APLICACIÓN BLOQUEADA	INTENTOS ACCESO
C:/Users//AppData/Local/Google/ GoogleUpdate.exe	7
C:/correos jhon/Mobogenie/mgusb.exe	5
C:/Program Files/Amazon Browser Settings/AmznSearchProtect.exe	4
C:/correos jhon/Mobogenie/UpdateMoboGenie.exe	2
C:/Program Files (x86)/Hewlett-Packard/HP Support Solutions/Modules/HPSFReport.exe	1
C:/SQLLIB/bin/db2jds.exe	1
C:/Program Files/CONEXANT/Flow/AppFollower.exe	1
C:/Program Files (x86)/Intel/Intel(R) Management Engine Components/LMS/LMS.exe	1
C:/instaladores/CERRA/CryptoServiceNet.exe	1
C:/Program Files/Synaptics/SynTP/SynTPEnh.exe	1
C:/Users//AppData/Local/GoToMeeting/86/g2mupdate.exe	1
C:/Program Files/Amazon Browser Settings/updater.exe	1
C:/Program Files (x86)/Intel/Intel(R) Management Engine Components/DAL/jhi_service.exe	1
C:/SQLLIB/bin/db2ccs.exe	1
Total general	**28**

RESULTADOS POLÍTICA DE CONTROL DE DISPOSITIVOS ESTACIONES

La directiva de control de dispositivos se creó con el fin de bloquear los medios extraíbles en las estaciones. En el siguiente gráfico se muestran los tipos de dispositivos que fueron bloqueados en tres últimos meses por medio de la política creada.

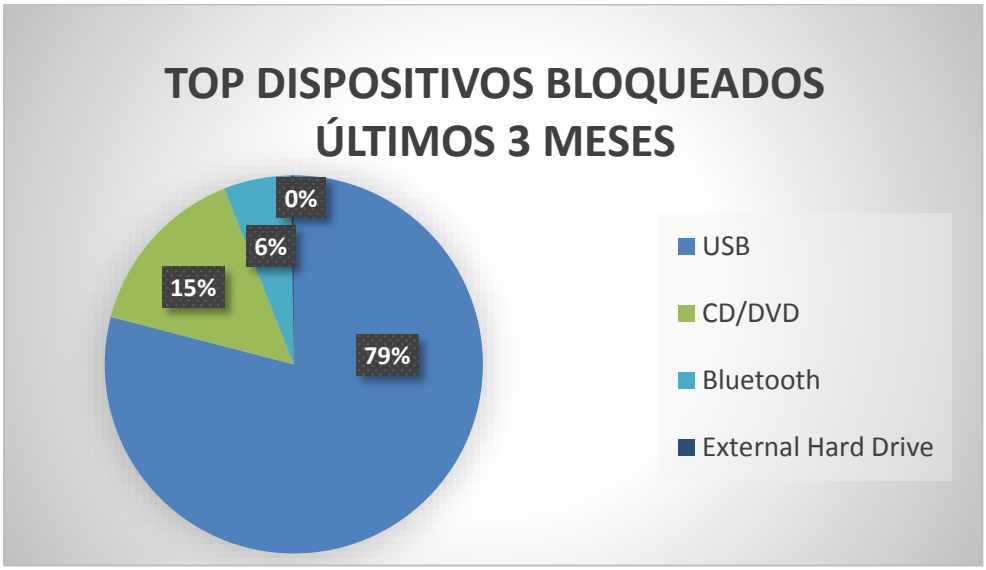


Figura 6.4: Top de Dispositivos bloqueados en los últimos 3 meses

En el siguiente listado se puede observar que el mayor intento de acceso a medios extraíbles fue el de USB, seguido del acceso a las unidades de CD/DVD.

Tabla 6.4: Dispositivos Bloqueados en los últimos 3 meses

TIPO DISPOSITIVO BLOQUEADO	CANTIDAD
USB	607
CD/DVD	115
Bluetooth	44
External Hard Drive	2
Total general	**768**

RESULTADOS POLÍTICA DE FIREWALL ESTACIONES

La directiva de firewall en estaciones se encuentra en la fase de piloto, en la cual se encuentra aplicada a una agencia.

La aplicación de la directiva se la está realizando de forma progresiva, debido a que en caso de que no se haya considerado algún acceso, la política denegará el servicio sobre la estación que utiliza dicha conexión. Cabe mencionar que las estaciones no se encuentran desprotegidas, dado que progresivamente se ha estado implementado los demás controles (antivirus, IPS, control de aplicaciones y dispositivos).

Por lo antes expuesto, aun no se tiene resultados de conexiones maliciosas bloqueadas a nivel de firewall de las estaciones.

RESULTADOS POLÍTICA DE PREVENCIÓN DE INTRUSOS ESTACIONES

La directiva de prevención de intrusos ha bloqueado en sus últimos 3 meses, un considerable número de vulnerabilidades en los equipos de los usuarios. En la siguiente tabla se indica el número de bloqueos realizados por la directiva de IPS en únicamente 6 meses, debido a que desde ese tiempo la política se encuentra vinculada en todas las 3.200 estaciones.

Tabla 6.5: Listado de Bloqueos realizados por el IPS los últimos 6 meses

Mes	Cantidad Intentos Bloqueados
Mes 1	76
Mes 2	171
Mes 3	46
Mes 4	111
Mes 5	130
Mes 6	52
TOTAL	**586**

Durante los primeros 6 meses posteriores a la aplicación de la directiva de prevención de intrusos, se han bloqueado 586 intentos de explotación de vulnerabilidades en las estaciones.

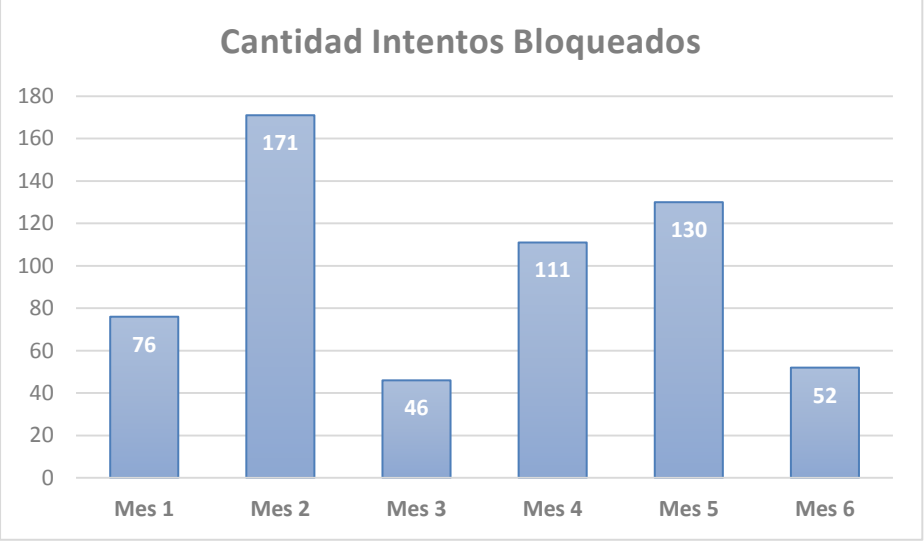


Figura 6.5: Intentos bloqueados por la política de IPS

En la Figura 6.6 y Tabla 6.6 se indican las vulnerabilidades más relevantes que fueron bloqueadas en las estaciones, referente a los últimos 6 meses:

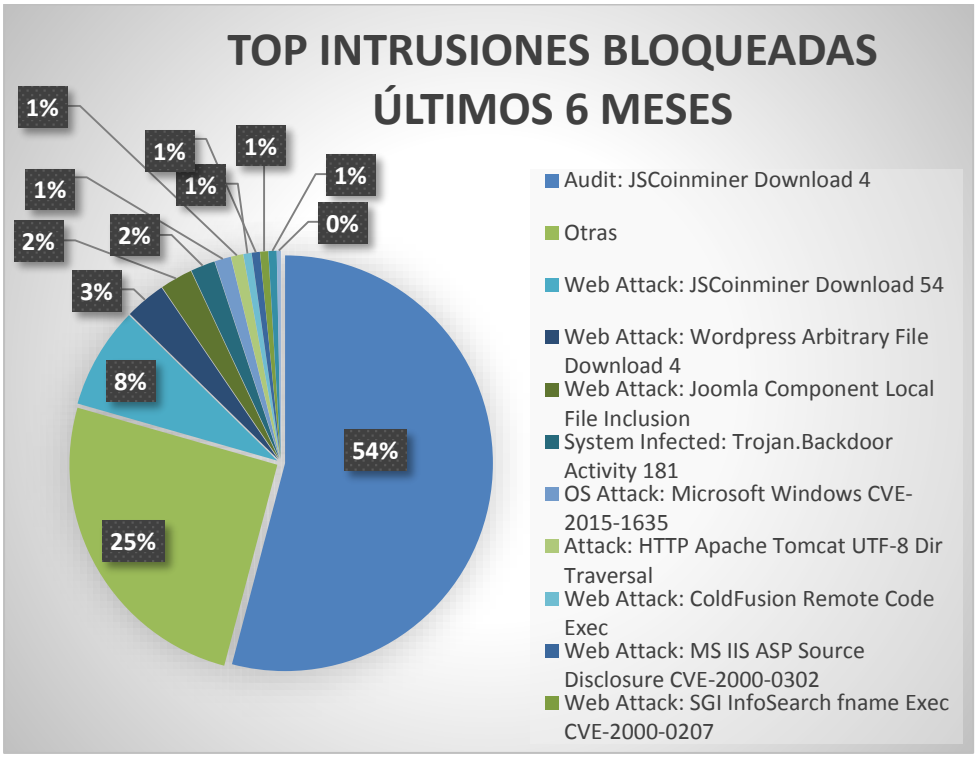


Figura 6.6: Top de intrusiones bloqueadas en últimos 3 meses

Tabla 6.6: Detalle de Vulnerabilidades Bloqueadas por el IPS

NOMBRE VULNERABILIDAD	CANTIDAD
Audit: JSCoinminer Download 4	171
Otras	80
Web Attack: JSCoinminer Download 54	25
Web Attack: Wordpress Arbitrary File Download 4	10
Web Attack: Joomla Component Local File Inclusion	8
System Infected: Trojan.Backdoor Activity 181	6
OS Attack: Microsoft Windows CVE-2015-1635	4
Attack: HTTP Apache Tomcat UTF-8 Dir Traversal	3
Web Attack: ColdFusion Remote Code Exec	2
Web Attack: MS IIS ASP Source Disclosure CVE-2000-0302	2
Web Attack: SGI InfoSearch fname Exec CVE-2000-0207	2
Web Attack: Wordpress Arbitrary File Download	2
Total general	**315**

RESULTADOS POLÍTICA DE INTEGRIDAD DE EQUIPOS

La directiva de integridad de equipos fue creada con la regla de verificación de la remediación de la vulnerabilidad MS17-010 y con la regla depuración de administradores locales no permitidos para lo cual se tiene los siguientes resultados de su cumplimiento:

- **Verificación de actualización KB4012215 a nivel de sistema operativo**

  Mediante la regla creada, se ha identificado que de las 3.200 estaciones que se tienen identificadas como activas, al momento se tienen 359 estaciones que no tienen aplicado el parche referente al boletín MS17-010.

Tabla 6.7: Detalle de Estaciones con el KB4012215 instalado

COMENTARIO KB4012215	CANT
Equipo Tiene Instalado KB4012215	2.841
Equipo No Tiene Instalado KB4012215	359
Total general	**3.200**

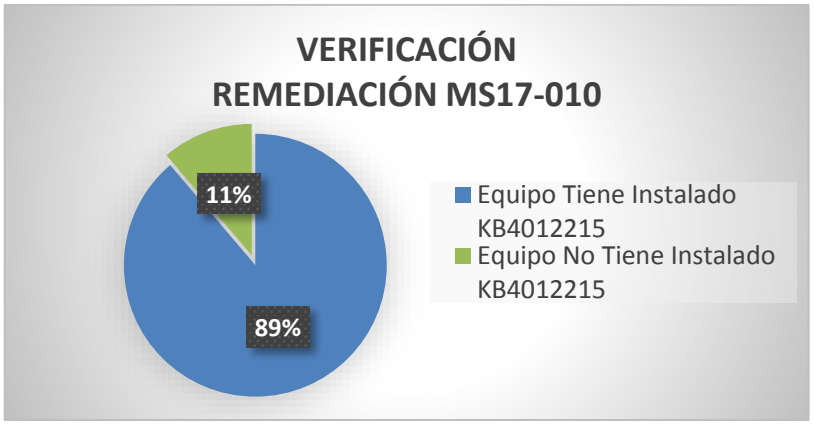


Figura 6.7: Verificación Remediación MS17-010

- **Depuración de Administradores locales no permitidos**

La regla de cumplimiento de depuración de administradores locales, nos ha dado la visibilidad de identificar cuando un administrador local no permitido se encuentra agregado.

En la siguiente tabla se puede observar que de las 3.200 estaciones declaradas como activas, únicamente 183 estaciones tienen administradores locales no permitidos (usuarios finales), debido a que las mismas son del área de sistemas, las cuales están siendo removidas progresivamente.

Tabla 6.8: Detalle Estaciones con administradores Locales Permitidos

COMENTARIO ADMINISTRADORES LOCALES	CANT
Equipo con Administradores Locales No Permitidos	183
Equipo sin Administradores Locales No Permitidos	3.017
Total general	**3.200**

Figura 6.8: Depuración de Administradores Locales No Permitidos

CONCLUSIONES Y RECOMENDACIONES

1. Al analizar la situación actual de la seguridad lógica de las estaciones, se detectaron los diferentes riesgos y vulnerabilidades que se encontraban en los equipos, consiguiendo de esta forma proponer un esquema de seguridad aterrizado a la realidad de la entidad financiera.
2. Se definieron los diferentes controles a implementarse y configurarse en el software de protección final, tomando como casos de uso las diferentes problemáticas presentadas en la situación inicial de la empresa.
3. El análisis de los diferentes requerimientos y aplicativos que son utilizados por los usuarios nos permitió tener una visibilidad de los componentes, comunicaciones, ejecutables y medios que podían verse afectados por la implementación del esquema de seguridad lógica propuesto.

4. Mediante el uso de una directiva de protección proactiva de antivirus se logró identificar archivos maliciosos que no eran detectados por la protección reactiva en base a firmas que estaban configuradas a nivel de estaciones.
5. La política de control de aplicaciones de SEP configurada a nivel de las estaciones, ayudó a restringir el acceso a aplicativos cuyo uso no se encontraba permitido por la empresa.
6. En la actualidad la directiva de control de aplicaciones aparte de ayudar a bloquear la ejecución de aplicaciones maliciosas, también ayuda a identificar a computadoras y usuarios que utilizan aplicaciones que no están licenciadas por la empresa, evitando de esta forma algún tipo de multa por los fabricantes de software.
7. Ciertos usuarios estaban acostumbrados a utilizar aplicativos cuya licencia no se encontraba adquirida, por lo que el avance de la aplicación de la directiva de control de ejecutables en dichos equipos se dificultaba, teniendo en ciertos casos que buscar herramientas que cumplan las mismas funcionalidades del aplicativo restringido y cuya licencia sea libre.
8. La directiva de control de dispositivos ayudó a administrar y monitorear los diferentes medios extraíbles que son conectados a los ordenadores, sin denegar el uso de equipos con interfaz USB que no cumplen la funcionalidad de almacenamiento de información.
9. Debido a la problemática que la entidad financiera tiene para realizar mensualmente la instalación de actualizaciones en las 3.200 estaciones debido al corto ancho de banda en sus sucursales y a equipos que se encuentran apagados, la directiva de prevención de intrusos nos ayudó a mitigar las diferentes vulnerabilidades que podrían ser aprovechadas por virus maliciosos en la red.
10. La aplicación de la directiva de firewall en las estaciones se la debe realizar de forma progresiva y controlada, debido a que en caso de que no se haya considerado algún acceso, la política denegará el servicio sobre la estación que utiliza dicha conexión.

Adicional a ello se debe priorizar la vinculación en sucursales y agencias, debido a que los aplicativos y conexiones son estándares en dichas localidades.

11. Mediante el uso de la directiva de integridad de equipos, se ha logrado identificar las estaciones que cumplen ciertos requerimientos de actualizaciones, los cuales son fundamentales para la remediación de ciertas vulnerabilidades detectadas.
12. Se ha logrado mantener exclusivamente los administradores locales permitidos en los equipos, mediante el uso de la funcionalidad en las reglas de integridad de equipos, la cual permite desplegar un script personalizado.
13. Se logró detectar una falla en la consola SEPM 12.1.5, a nivel del módulo de control de aplicaciones, el cual generaba una lentitud y un alto consumo de CPU del servidor, el cual se producía porque la consola no soportaba el enmascaramiento de las rutas de instalación de aplicativos. Meses posteriores, el fabricante publicó la respectiva actualización de la consola, corrigiendo lo reportado en la versión SEPM 14.1.0.

RECOMENDACIONES

1. Se debe monitorear el buen funcionamiento de todos los clientes de antivirus en las máquinas, debido a que si los mismos se encuentran con inconvenientes, los controles implementados no serían cubiertos en dichas estaciones de forma óptima.
2. Realizar un programa de capacitación para los usuarios, para que lo mismos no respondan correos a de dudosa procedencia, no accedan a links adjuntos, no descarguen archivos adjuntos de desconocidos, ejecuten aplicaciones de dudosa procedencia, esto con el objetivo de reducir la cantidad de infecciones por correos maliciosos.
3. Explotar en su máxima capacidad las directivas de integridad de estaciones, debido a que las mismas ofrecen una gran variedad de tareas y acciones que pueden ser tomadas como parte complementaria para el aseguramiento lógico de las estaciones.
4. Actualizar las reglas de control de ejecución de aplicaciones, con la finalidad de reemplazar las rutas de instalación de los ejecutables por el respectivo hash SHA256 del aplicativo, reduciendo de esta forma el campo de acción de los archivos maliciosos.
5. Verificar constantemente las firmas de IPS publicadas por el fabricante, a fin de que las mismas puedan ser habilitada en modo de bloqueo, reduciendo de esta forma la explotación de las vulnerabilidades reportadas en los boletines.

BIBLIOGRAFÍA

[1] El Financiero, Bancos acuerdan 5 puntos para proteger tu información financiera, http://www.elfinanciero.com.mx/empresas/bancos-acuerdan-puntos-para-proteger-tu-informacion-financiera.html, fecha de consulta Enero 2018.

[2] TechNet Microsoft, Protección de los equipos cliente contra los ataques de red, https://technet.microsoft.com/es-es/library/cc875823.aspx, fecha de consulta Enero 2018.

[3] Privacy Rights Clearinghouse, Cómo proteger su computadora y su privacidad, https://www.privacyrights.org/c%C3%B3mo-proteger-su-computadora-y-su-privacidad#c%C3%B3mo-usar-su-computadora-de-forma-segura, fecha de consulta Enero 2018.

[4] United States Computer Emergency Readiness Team, Understanding Anti-Virus Software, https://www.us-cert.gov/ncas/tips/ST04-005, fecha de consulta Febrero 2018.

[5] Symantec, Protección de endpoints contra las amenazas persistentes avanzadas con Symantec Endpoint Protection 12.1, http://www.symantec.com/content/es/mx/enterprise/white_papers/Advanced-Protection-with-SEP12-v1-SL.pdf, fecha de consulta Febrero 2018.

[6] Real Academia Española, Definición de heurístico, http://dle.rae.es/srv/fetch?id=KHdGTfC, Fecha de consulta Enero 2018.

[7] Symantec, Acerca de SONAR, https://support.symantec.com/es_ES/article.HOWTO80968.html, Fecha de consulta Febrero 2018.

[8] Symantec, Symantec Endpoint Protection Application and Device Control, https://www.symantec.com/security_response/securityupdates/list.jsp?fid=adc, Fecha de consulta Abril 2018.

[9] Symantec, Acerca del firewall de Symantec Endpoint Protection, https://support.symantec.com/es_ES/article.HOWTO80961.html#v42226922, Fecha de consulta Abril 2018.

[10] Symantec, Configuración de reglas de firewall, https://support.symantec.com/es_ES/article.HOWTO98492.html, Fecha de consulta Abril 2018.

[11] Kenneth C. Laudon, Sistemas de información gerencial: Administración de la empresa digital, https://books.google.com.ec/books?hl=es&lr=&id=KD8ZZ66PF-gC&oi=fnd&pg=PA210&dq=aplicativos+internos+empresa&ots=hlkiq5jW0D&sig=DKfry8PvDB8m-H8yBd9jH7Y9tAQ#v=onepage&q=aplicativos%20internos%20empresa&f=false, Fecha de consulta Abril 2018, Página 212.

[12] Jane Price Laudon, Sistemas de información gerencial: Administración de la empresa digital, https://books.google.com.ec/books?hl=es&lr=&id=KD8ZZ66PF-gC&oi=fnd&pg=PA210&dq=aplicativos+internos+empresa&ots=hlkiq5jW0D&sig=DKfry8PvDB8m-H8yBd9jH7Y9tAQ#v=onepage&q=aplicativos%20internos%20empresa&f=false, Fecha de consulta Abril 2018, Página 214.

[13] Symantec, About the default Virus and Spyware Protection policy scan settings, https://support.symantec.com/en_US/article.HOWTO80937.html, Fecha de consulta Mayo 2018.

[14] Symantec, Wannacry 2.0, https://www.symantec.com/connect/forums/wannacry-20, Fecha de consulta Mayo 2018.