Diseño de un esquema de seguridad informática para PYMES, como la primera línea de defensa para la protección contra amenazas de Ransomware, utilizando los lineamientos de la norma ISO27001:2013

Tatiana Montoya Correa

Andrés Molano Luján

Ingeniería en Telecomunicaciones

Leonardo Serna

INSTITUTO TECNOLÓGICO METROPOLITANO

2017

RESUMEN

Debido a la evolución acelerada de la tecnología, se vienen presentando vulnerabilidades en los esquemas de seguridad de las organizaciones, ya que en algunos casos no se encuentran bien definidas las políticas de seguridad. Estas amenazas pueden ser explotadas, ya sea para sacar un beneficio económico o simplemente para hacer un daño irreparable a la información.

Existen ataques a nivel de red local, es decir, ataques dirigidos a la infraestructura interna de la empresa. Para remediar esto existe una serie de políticas y dispositivos para mitigar los riesgos de seguridad de la información. Otro escenario sería aquel en el que los empleados se llevan los equipos a sus casas o a otra locación y, en este caso, las políticas que se aplicaron en el equipo de protección del perímetro (por ejemplo: Firewall de red, UTM), no cubriría a estos equipos puesto que no se encuentran dentro en la red protegida, las políticas de equipos que pertenezcan a dominios Windows seguirán siendo aplicadas, pero no cubrirán la totalidad de la seguridad. Es por esto, que también se debe proteger los dispositivos a nivel de Endpoint (host o usuario final), lo que significa que serán protegidos en cualquier lugar en que se encuentren. Cuando los equipos retornen a la red recibirán las actualizaciones de políticas que se hayan modificado.

La realización de este trabajo de grado consta de una guía de políticas y procedimientos que brinda a las pymes controles de seguridad informática a nivel de red y nivel de host, para proteger su información de amenazas de Crypto Ransomware. El diseño se realizará implementando políticas de seguridad a través de dispositivos perimetrales y herramientas de software; además, se tomarán para los procedimientos de un plan de recuperación ante Crypto Ransomware, los lineamientos del estándar internacional del sistema de gestión de seguridad ISO27001:2013, enfocados en el dominio de control A17 sobre protección y continuidad de negocio.

RECONOCIMIENTOS

A Dios, por

Habernos permitido llegar hasta este punto y dado salud para lograr nuestros objetivos, además de su infinita bondad y amor.

A nuestras familias, por

Habernos apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que nos ha permitido ser personas de bien, pero más que nada, por su amor.

A todos aquellos quienes de una u otra manera nos alentaron a seguir adelante, por medio de sus actitudes motivacionales.

ACRÓNIMOS

UTM Unified Threat Management

ISO International Organization for Standardization

IEC International Electrotechnical Commission

TI Tecnologías de la información

WAN Red de área amplia

LAN Red de área local

IPS Sistema de prevención de intrusiones

IDS Sistema de detecciones de intrusiones

PYME Pequeña y mediana empresa

SSL Secure Sockets Layer

HIPS Sistema de prevención de intrusiones basado en host

TCP Protocolo de Control de Transmisión

IP Protocolo de internet

OSI Open System Interconnetion

PC Computador personal

URL Localizador Uniforme de Recursos

VPN Red privada virtual

NIDS Network Intrusion Detection System

HIDS Host-based Intrusion Detection System

CIFS Common Internet File System

NFS Network File System

USB Universal serial bus

CD Disco compacto

DVD Disco versátil digital

SA Servidor de archivos

PR Plan de recuperación

TABLA DE CONTENIDO

1. INTRODUCCIÓN

1.1 . GENERALIDADES

El área de las tecnologías de la información adquiere cada día mayor importancia en el crecimiento de las organizaciones y en la eficacia de las operaciones que se realizan en éstas. Para que las empresas puedan soportar las necesidades de los usuarios en sus diferentes áreas, debe realizar inversiones, tanto a nivel de hardware como de software; migrando todos sus procedimientos manuales a plataformas que pueden realizar estas tareas de manera más eficiente. De esta forma, se empiezan a manejar grandes flujos de información que son esenciales en la dinámica de la empresa, ubicando los datos como el activo más importante que poseen las organizaciones.

Las PYMES, a la hora de invertir en su infraestructura tecnológica, asumen como última opción la inversión en seguridad, pues tienen la percepción de que es un gasto que pueden evitar, y no dimensionan las consecuencias negativas que puede tener en la continuidad de su negocio; no tienen diseñados políticas y procedimientos de preparación y contingencia ante una eventualidad en el acceso a su información y, cuando realizan inversiones en este campo en muchas ocasiones adquieren hardware de seguridad, pero no tienen un personal capacitado para que implemente políticas adecuadas en estos equipos. Según el informe anual de McAfee Labs sobre las amenazas para 2016," como cualquier otro activo de valor, la información también atrae la atención de los ciberdelincuentes " (labs, 2016). Es por esto, que se debe tomar la protección de los datos como parte esencial a la hora de la inversión de recursos en el área de tecnología.

Existen diferentes tipos de malware que afectan los sistemas informáticos, pero desde principios de 2015 (Kevin Savage, 2015). Viene tomando gran crecimiento una amenaza que, a pesar de no ser nueva, causa un gran impacto negativo tanto en pequeñas como en

grandes empresas. Este es el llamado Ransomware. Es un tipo de malware que se caracteriza por encriptar cierto tipo de archivos, en la mayoría de ocasiones son los archivos más utilizados por los usuarios, como documentos de Word, Excel, Pdf entre otros. Y ha tomado gran popularidad, dado que, al infectar el equipo del usuario, encripta los datos que se encuentren en el computador, y además pide un rescate a cambio para que el usuario propietario de la información pueda acceder a ésta nuevamente. Dicha amenaza, al utilizar tipos de cifrado complejo, hace prácticamente inutilizable la información. Al poner esta amenaza en un ambiente corporativo de una pequeña empresa, donde no se tenga el conocimiento necesario para combatir este tipo de malware y no se apliquen las políticas y los procedimientos adecuados, se verían comprometidos datos valiosos y la continuidad del negocio.

1.2 OBJETIVO GENERAL

Diseñar guía de políticas y procedimientos en seguridad informática para ser implementada en PYMES, como primera línea de defensa para la protección ante amenazas Crypto Ransomware, que puedan comprometer la integridad y disponibilidad de los datos.

1.3 OBJETIVOS ESPECIFICOS

- Diseñar las políticas de configuración aplicables a dispositivos perimetrales con su respectiva documentación para la protección a nivel de red que permitan mitigar los riesgos de Crypto Ransomware.

- Diseñar las políticas de configuración adecuadas de una consola de seguridad Endpoint con su respectiva documentación para la protección a nivel de host que permitan mitigar los riesgos de Crypto Ransomware.

- Proponer un procedimiento de recuperación post-incidente ante una infección de Crypto Ransomware que comprometa la integridad o la disponibilidad de la información de un servidor de archivos en una PYME.

- Proponer un mapeo de las políticas y procedimientos diseñados indicando los controles tenidos en cuenta del dominio A17 del anexo A de la norma ISO27001:2013.

1.4. ORGANIZACIÓN DEL TRABAJO

FASE I: Parte de una idea inicial, la cual fue dividida en varios objetivos específicos y una justificación para el desarrollo del trabajo.

FASE II: Recolección de documentación, utilizando los artículos publicados por expertos en seguridad y las empresas más representativas de la industria de la seguridad informática

FASE III: Una vez se cuenta con la fundamentación teórica para el entendimiento del trabajo, se inicia con la ejecución de objetivos, el diseño de esquemas y la propuesta de políticas y procedimientos

FASE FINAL: La parte final del proyecto consta de las conclusiones, donde se analiza el alcance que podrán tener las políticas y procedimientos planteados a los lectores del trabajo**;** también se plantea una serie de recomendaciones para futuras entregas.

2. MARCO TEÓRICO

2.1 . SEGURIDAD INFORMÁTICA

Se define como el aseguramiento de los recursos informáticos de una organización o de individuos que posean datos o material informático. El acceso a esta información debe ser protegido para que sólo las personas autorizadas puedan tener acceso a ver o modificar estos datos. Existen 3 conceptos y pilares básicos para poder comprender la seguridad informática, los cuales son la **disponibilidad, integridad y confidencialidad**.

Disponibilidad: Es una característica que identifica a un sistema, datos o servicios, para que estos puedan ser accedidos por usuarios o procesos al momento que lo necesiten; va también relacionado con los procesos de recuperación de información en el momento de ser requeridos. Es importante reconocer que no sólo se debe contar la información íntegra y segura, sino que también es fundamental disponer de ella para ser consultada cuando el sistema involucrado lo crea necesario.

Integridad: Es la cualidad que poseen los datos o archivos que no han sido modificados. Además, puede ser comprobada su autenticidad, debido a que el archivo original no ha recibido ninguna alteración durante la transmisión; esta se puede comprobar con ayuda de funciones como los hash.

Los hash son funciones matemáticas que permiten, a través de procesos criptográficos, crear, mediante una entrada (ya sea un archivo, texto o contraseña), una cadena alfanumérica que sólo puede ser replicada con exactamente los mismos datos a la entrada

de la función. Por medio de estas funciones el destinatario podría obtener la comprobación de que el mensaje no ha sido modificado.

Confidencialidad: Es una característica que debe tener un archivo o recurso informático, para que sólo el personal autorizado pueda tener la capacidad de entender su contenido y poder utilizarlos según sea su fin. "En el caso de un mensaje esto evita que exista una intercepción de éste y que pueda ser leído por una persona no autorizada" (Santos, 2011).

Por lo tanto, el proceso de cifrado permite obtener un nivel de seguridad que consiste en la alteración del mensaje original, para que este no sea entendible por una parte ajena al sistema receptor involucrado. Existen 2 tipos de cifrado en el área informática: los simétricos y asimétricos.

En el caso del sistema simétrico se entiende por el tipo de cifrado que contiene una clave conocida por ambos extremos (el emisor y el receptor); ésta será usada, tanto para el encriptado como para el desencriptado de los datos; este tipo de cifrado tiene un inconveniente: no existe una manera segura de transmitir la clave de un extremo a otro, dado que los dos extremos deben conocerla y sólo quien la genera la conoce. Además, como principio de seguridad, se debe renovar de manera constante dicha clave.

El otro tipo de cifrado es conocido como asimétrico. Cada extremo de la comunicación cuenta con 2 claves de cifrado: una pública, la cual está disponible para cualquier usuario, y una privada, que se mantiene en custodia de forma que sólo el receptor la pueda conocer. El mensaje desde un extremo que sea cifrado a través de la clave pública podrá ser descifrado únicamente con la clave privada y viceversa. Aunque exista relación entre estas dos claves, no podrá conocerse una a partir de la otra. Uno de los inconvenientes del cifrado asimétrico es que los algoritmos usados son más complejos y requieren mayor procesamiento computacional.

En la tabla 1 se realiza una explicación básica de 3 conceptos de la seguridad de la información, Disponibilidad, integridad y confidencialidad. En el campo ataques se muestran algunos ejemplos de actividades que podrían afectar el cumplimiento de los objetivos del criterio seleccionado. La disponibilidad puede ser afectada por ataques de denegación de servicio, la integridad puede perderse por la modificación no permitida de los datos y la confidencialidad puede ser vulnerada por la intercepción de mensajes de manera fraudulenta.

Otro campo ilustrado son las consecuencias que podría acarrear un ataque, en la disponibilidad se podría perder totalmente la funcionalidad del sistema, al perder la integridad el sistema podría presentar datos erróneos o un atacante podría mostrar información falsa a los usuarios, el tercer ítem la confidencialidad muestra que su degradación permitiría que personas no autorizadas accedan a información sensible que es de uso privado.

El ultimo campo muestra algunas técnicas de protección que ayudarían a preservar el objetivo principal de los criterios seleccionados, Para conservar la disponibilidad existen sistemas a prueba de fallos que cuando uno queda sin servicio, el siguiente toma sus funciones, existen técnicas de Hashing y firma digital para asegurar que el mensaje enviado ,es el mismo que se recibe ,por último el cifrado de datos permite que los datos sean confidenciales y solo sean vistos por las personas que tienen este derecho.

Criterio	Ataques	Consecuencias	Técnicas de protección
Disponibilidad	Denegación de servicio	El sistema deja de funcionar	Sistemas tolerantes a fallos
Integridad	Modificación	Se trabaja con información incorrecta, ya sea simplemente errónea o malintencionada	Hashing Firma digital
Confidencialidad	Intercepción de mensajes	Personas no autorizadas pueden	Cifrado

		acceder a información confidencial	

Tabla 1. Tabla de conceptos de la seguridad. Fuente Autores

2.2. AMENAZAS INFORMÁTICAS

Una amenaza informática es todo elemento o acción capaz de atentar en contra de la seguridad de la información. Las amenazas a un sistema de información pueden originarse de varias fuentes:

- Amenazas internas: se generan al interior de la organización o de manera externa, tienden a causar gran daño debido a que los usuarios cuentan con acceso directo a la información e infraestructura. Este tipo de amenazas ocurren en el momento que un empleado por accidente o de manera intencional realiza manejo inadecuado de la información sensible, también pueden ocurrir por medio de unidades externas infectadas o proporcionando acceso mediante infecciones provenientes de correos electrónicos.

- Amenazas externas: ocurren cuando personal que no pertenece a la organización como por ejemplo Ciberdelincuentes, descubren los vacíos de seguridad y consiguen acceso a la red interna a través de malware o ataques dirigidos.

Las personas son los principales vectores de ataque a los sistemas de información, ya sea con o sin intención; y serán quienes pueden llegar a generar grandes pérdidas en los sistemas que se necesitan proteger. El objetivo principal de aquellas personas que quieren ingresar de manera fraudulenta a un sistema es obtener el máximo nivel de privilegio posible. Es poco común que el personal de seguridad tenga en cuenta factores como la ingeniería social al momento de crear políticas de protección a sus datos, dando con esto herramientas a piratas informáticos y a personas no deseadas.

Es importante reconocer que cada uno de los empleados de una organización afecta de manera directa la seguridad de un sistema, pues ellos tienen a la mano todos los recursos y son quienes manipulan día a día los datos. Luego de que un empleado abandona la organización, en algunos casos las cuentas con los que ingresaban al sistema permanecen activas por meses, lo que permite el acceso no autorizado a información que ya no hace parte de sus funciones.

Existen tipos de personas que simplemente intentan vulnerar el sistema de manera pasiva, es decir, sólo acceden por curiosidad; otro tipo de personas más peligrosas son los piratas informáticos, que tienen gran conocimiento en las áreas informáticas y pueden ser pagados por terceros para robar información sensible o inhabilitar sistemas de compañías rivales.

2.3. MALWARE

Es cualquier tipo de programa o archivo perjudicial para dispositivos informáticos, algunos tipos de malware incluyen virus de computadoras, spyware, troyanos, Ransomware, gusanos, rootkits, entre otros. El objetivo de este tipo de software es infectar el dispositivo para tomar el control y realizar funciones como robo de identidades, envió de correo spam, ataques de denegación de servicio, cifrado y eliminación de datos sensibles, y monitoreo a la actividad del usuario en ese equipo.

En el ambiente informático los tipos de malware se identifican por tener características específicas. Un gusano es una clase de malware que puede replicarse entre dispositivos, sin necesidad de interacción humana para esto. Un virus es un programa malicioso que se caracteriza por infectar programas o archivos. Un troyano es un tipo de infección que se hace pasar por un programa legítimo para tomar el control de la máquina. El malware tipo

spyware, que tiene como función recopilar información y datos, sin conocimiento de los usuarios.

En 1990 fue usado por primera vez el término de malware por el científico informático Yisrael Radai. Al principio, el uso de este tipo de software malicioso era usado generalmente por jóvenes aficionados con fines de diversión y con el objetivo de conocer hasta dónde era posible que se propagaran. En la actualidad se desconoce la cantidad de malware que existe e, incluso, ha llegado a pensarse que se ha creado más malware que software.

2.4. RANSOMWARE

Con la expansión de la conectividad en internet y la distribución de datos sensibles en estaciones de trabajo, se proveen opciones de acceso remoto baratas y de bajo riesgo, contra los intrusos. En 2015, el top 6 de países afectados por malware fueron Estados unidos, Japón, Reino Unido, Italia, Alemania y Rusia; los cuales han realizado un promedio de pagos por rescate de información de USD 300 dólares (Kevin Savage, 2015). Por esto, se ha hecho cada vez más necesario contar con una protección adecuada para contrarrestar la cantidad de malware existente, que está en constante crecimiento a la par con los sistemas y aplicaciones.

A principios de 2005 inicia La primera ola de Ransomware (software de secuestro digital) moderno con un malware denominado Trojan Gpcoder. Este es un tipo de troyano busca archivos que contiene varias extensiones, y los codifica; luego, los archivos originales son eliminados y los nuevos quedan ilegibles (Kevin Savage, 2015). Posteriormente, el usuario final para poder recuperar sus datos deberá pagar cierta cantidad de dinero.

Ransomware cuenta con múltiples variantes, entre los 5 Tipos más comunes se encuentran los siguientes: **cifrado** siendo el tipo más común, está diseñado para encontrar archivos valiosos almacenados en las computadoras de los usuarios, y realizar un proceso

de encriptación donde no podrán ser recuperados sin su respectiva clave de cifrado, **cifrado y borrado** este esta es similar al anterior con la diferencia que se van eliminando los datos de forma gradual sin solicitar algún rescate, **secuestro** su objetivo es el robo de la información solicitando un rescate para evitar que los datos robados sean públicos **, bloqueo** está diseñado para denegar el acceso al equipo del usuario final, bloqueando el ingreso a la interfaz que normalmente accede el usuario. En pantalla, solo se mostrará el portal donde se ingresa el código de desbloqueo y **espía** actúa espiando las actividades realizadas por el usuario en el equipo**.** Así, pues, con el crecimiento de las compañías y la tecnología, la información se ha convertido en pilar fundamental para la ejecución de labores diarias, y en ocasiones no se dimensiona la cantidad de vulnerabilidades a las que se está expuesto.

2.4.1.¿CÓMO FUNCIONA CRYPTO RANSOMWARE?

Existe gran cantidad de amenazas informáticas en los ambientes corporativos, entre las cuales se encuentran los gusanos, troyanos, phishing, entre otros. Recientemente ha ingresado a este ambiente una nueva amenaza llamada Crypto Ransomware, que consiste en el secuestro de información por parte de los ciberdelincuentes; esta información es cifrada y se pide un rescate a cambio para que pueda ser recuperada.

El Crypto Ransomware es un tipo de malware que se aprovecha de las vulnerabilidades que pueda tener un equipo para ingresar en éste. Una de las técnicas utilizadas es el Phishing, donde el ciberdelincuente se hace pasar por un usuario o una empresa de confianza a través de un correo electrónico, y así el usuario final será quien descargue el malware en el equipo afectado y poder realizar el proceso de encriptación (Medina, 2016). Los principales archivos atacados son aquellos en los que el usuario puede tener información más valiosa; algunos de estos archivos lo conforman las siguientes extensiones .zip, .jpg, .key, .mdb, .Pdf,.txt, .doc, .rtf, .ppt,. Luego de realizar este proceso, se envía un correo electrónico; o, al abrir estos datos, una ventana emergente se abre con

el mensaje que exige un pago a cambio de la clave de cifrado para poder recuperar la información (Liao).

Son varios los métodos con los cuales los ciberdelincuentes pueden procesar la información de la víctima: el primero consiste en comprimir los archivos en un .ZIP; luego, establecer una contraseña y eliminar los archivos originales. El segundo consiste en crear una carpeta oculta y mover allí los archivos. Este sería el método menos destructivo para el usuario, ya que le información sería recuperable. El tercer método consiste en encriptar la información utilizando un algoritmo de cifrado sofisticado como RSA. En este caso, por ejemplo, un archivo llamado trabajo1.doc pasaría a tomar el nombre de Encrypted_trabajo1.doc y sólo se podría abrir con su respectiva clave de cifrado. En la misma carpeta donde fueron cifrados los datos se creará un documento que contiene la información acerca del pago del rescate y la suma que se debe pagar. En la siguiente tabla se muestran algunas de las variantes que tiene el Ransomware, dando una breve descripción sobre su modo de actuar.

Nombre	Año	Método de ataque	Método de rescate
Trojan pluder.a	2006	Copia archivos a carpetas ocultas	Enviar 10 dólares a un banco chino
Arhiveus	2006	Enlaza todos los archivos de la carpeta "Mis Documentos "a un solo archivo con nombre EncryptedFiles.als y elimina todos los archivos originales. Crear un archivo de texto denominado "Instrucciones de cómo obtener sus archivosBACK.txt	Pide a las víctimas a comprar $ 75 en productos farmacéuticos de ciertos sitios web rusos.
Trojan.Randsom.A	2006	Cada 30 minutos Aparece una pantalla que indica, un archivo está siendo eliminado, aunque no es cierto	Exige un pago de $10 dólares a través de western unión
Trojan.Cryzip	2006	Comprime documentos (txt, doc, rft, etc.), en un archive ZIP protegido por contraseña.	Exige un pago de $300 dólares

Trojan.PGPCode	2005	Encripta todos los archivos usando un algoritmo RSA	Exige un pago de $200 dólares a través de una cuenta E-GOLD
Cute Ransomware	2016	Utiliza Google Docs para transmitir las llaves de cifrado y recoger información de los usuarios.	A través de pago con bitcoins
TeslaCrypt	2015	TeslaCrypt se dirige a archivos asociados a juegos y plataformas como RPG Maker, League of Legends, Call of Duty, Dragon Age, plataformas de juegos online.	Utiliza la plataforma paypal
WannaCry	2017	WannaCry ataca las vulnerabilidades de Windows por sistemas que no están actualizados.	Exige un pago de $300 dólares en bitcoins

Tabla 2. Modalidades de ataques Ransomware. Fuente Autores

2.4.2. MODO DE OPERACIÓN CRYPTO RANSOMWARE

Para la operación de Crypto Ransomware es necesario la interacción directa del usuario. A continuación, se describe el flujo de trabajo de una infección Crypto Ransomware:

1. El usuario recibe un correo electrónico que contiene una URL o un archivo adjunto que parece ser de procedencia confiable.

2. El usuario da click en la URL maliciosa, o descarga y ejecuta el archivo adjunto.

3. El archivo ejecutado inicia una serie de procesos donde descarga el binario que contiene el malware, y se instalara en la maquina afectada.

4. Inicia la etapa de encriptación, donde los archivos más usados por el usuario serán encriptados.

5. Luego, el malware envía la llave de encriptación a un servidor de comando y control.

6. En el equipo del usuario se muestra un mensaje donde se exige el pago de una cantidad de dinero, para poder recibir la clave de desencriptado de información.

En la siguiente figura se evidencia el ciclo de una infección Crypto Ransomware.

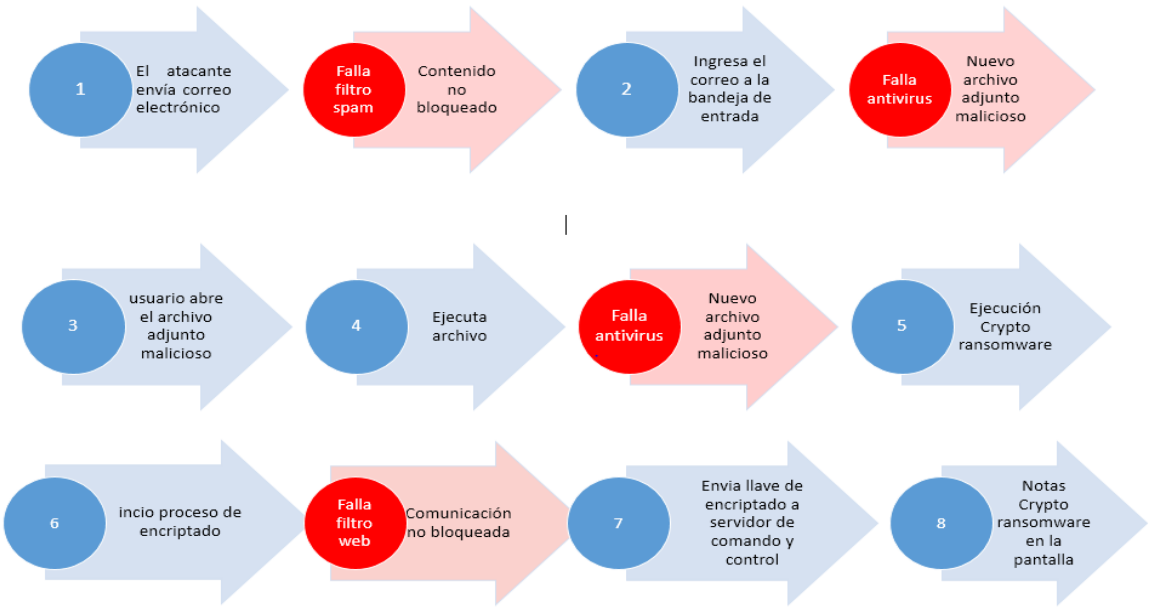

Figura 1 .Ejemplo de infección de crypto Ransomware. Fuente Autores

2.4.3. Ejemplo de Infección por Crypto Ransomware

A continuación, se muestra un ejemplo de infección de archivos afectados por una variante de Crypto Ransomware.

1. Un usuario común en la red de una empresa se dispone a trabajar con archivos de Word que se encuentran almacenados en un servidor de archivos.

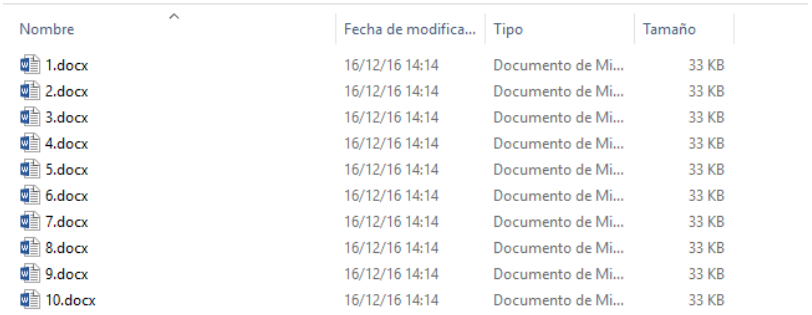

Figura 2. Archivos de Word. Fuente Autores.

2. El usuario recibe un correo electrónico en su equipo; este contiene un mensaje que lo persuade para que abra el archivo.

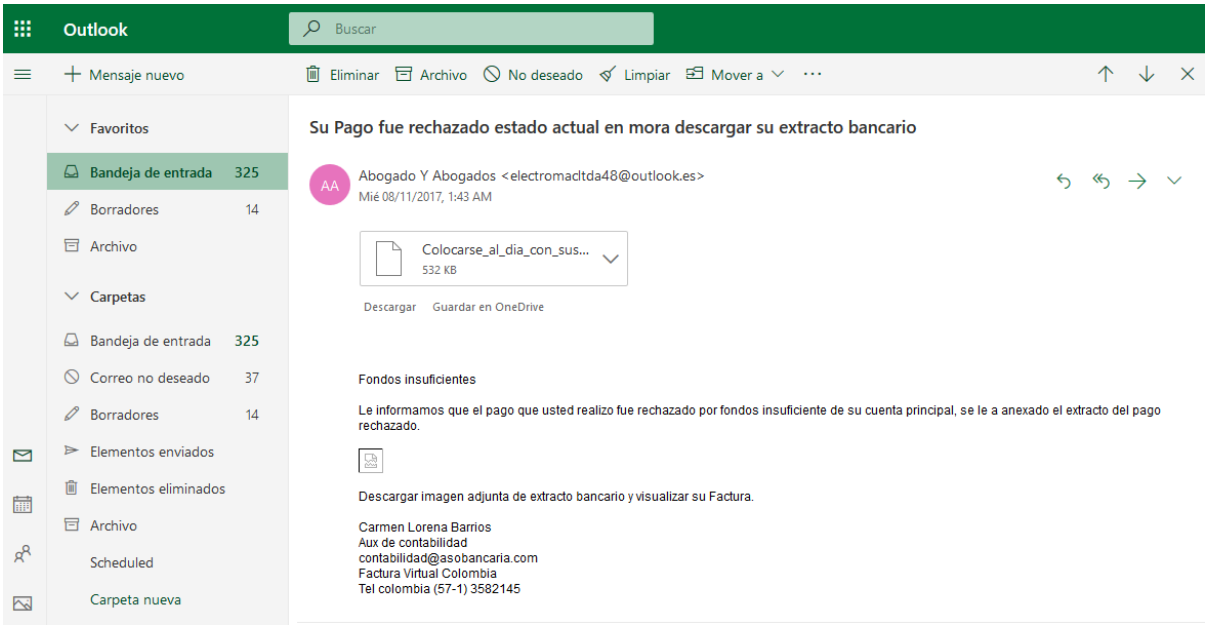

Figura 3. Correo electrónico sospechoso. Fuente Autores.

3. El usuario descarga y abre un archivo en formato .rar

Figura 4. Descarga archivo adjunto correo electrónico. Fuente Autores.

4. El usuario ingresa a la carpeta y ve un ícono aparentemente normal, y procede a dar clic para abrir el archivo.

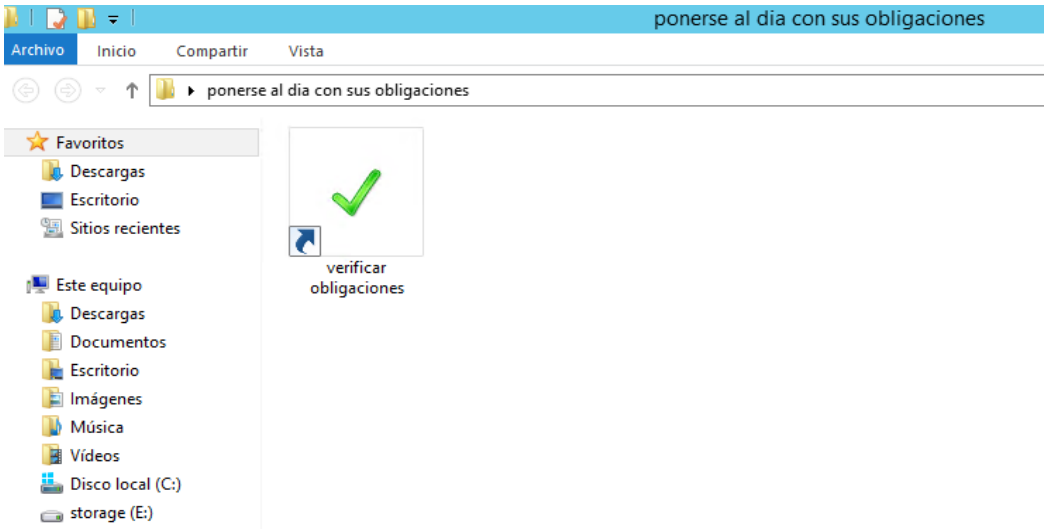

Figura 5. Contenido de la carpeta. Fuente Autores.

5. El usuario no se percata de que existen otros archivos ocultos en esta carpeta.

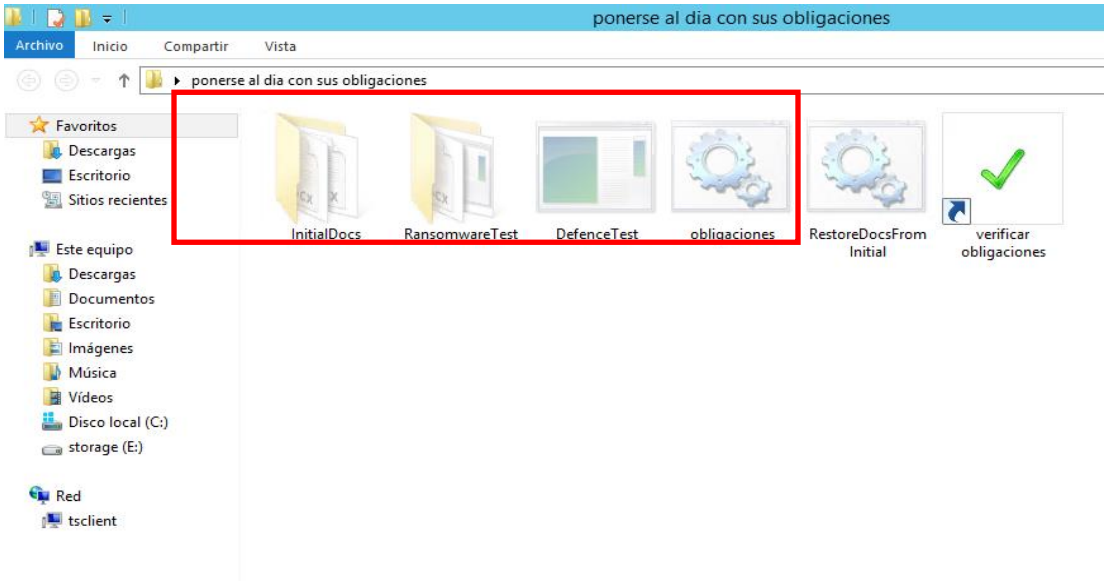

Figura 6. Archivos ocultos. Fuente Autores.

6. Una vez el usuario dio clic sobre el archivo, se inicia un proceso oculto que da inicio a la encriptación de los archivos y posterior pérdida de éstos.

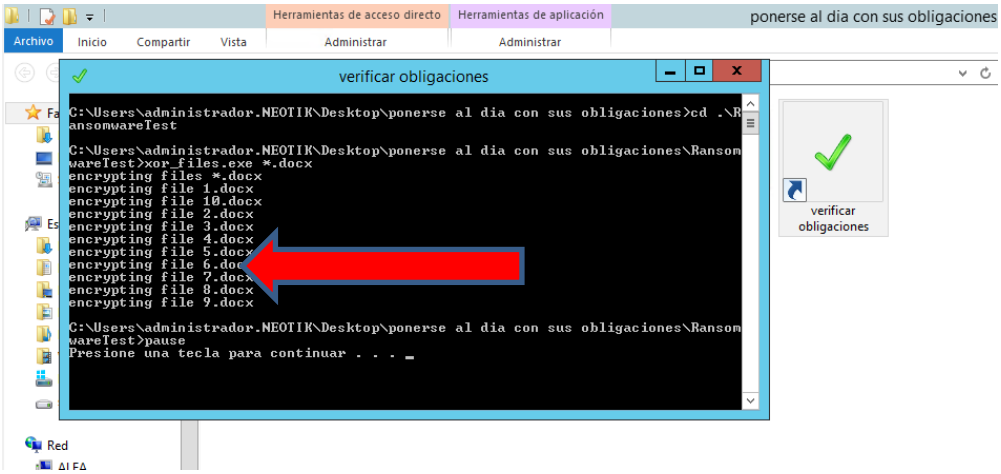

Figura 7. Proceso de encriptación. Fuente Autores.

7. Cuando el usuario desea trabajar sobre sus archivos, se percata de que éstos tienen una extensión totalmente diferente, y no puede acceder a ellos.

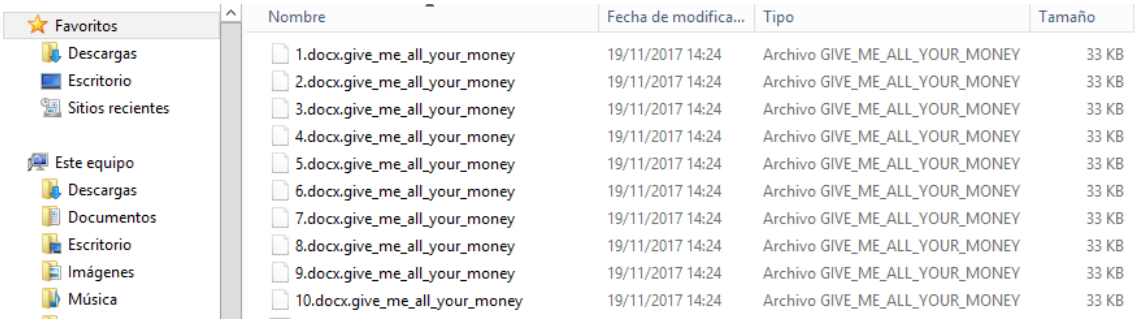

Figura 8. Archivos encriptados. Fuente Autores.

8. En este punto, todos los datos de Word que tenía almacenados el usuario han perdido su integridad, y la única manera de recuperarlos es accediendo al pago de la suma que exige el ciberdelincuente.

2.4.4. TENDENCIAS ACTUALES

Durante mucho tiempo Cerber ha sido la familia de Ransomware que más se ha propagado por el mundo, a mediados del mes de mayo de 2017 WannaCry ingreso en las redes a través de un gusano que explotaba una vieja vulnerabilidad de Windows. Durante ese mismo periodo Microsoft lanzo un parche para un error en el protocolo SMB, el cual permite a las computadoras compartir archivos e impresoras a través de la red local. Para el mal de varias empresas, estas no instalaron el parche y dejaron la puerta abierta para explotar esta vulnerabilidad a WannaCry que represento más del 45% de todo el Ransomware entre los meses de abril y octubre, en la figura 9 se puede observar la Tendencia de Ransomware en el periodo comprendido entre abril y octubre de 2017 .

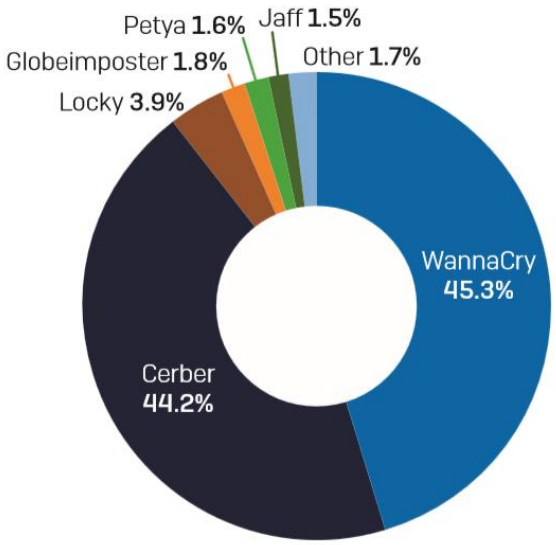

Figura 9. Tendencia de Ransomware en el periodo comprendido entre abril y octubre de 2017.Fuente "SophosLabs 2018 Malware Forecast".

WannaCry no era el tipo de Ransomware común que llegaba a través de un correo electrónico como enlace o archivo adjunto, por eso tuvo tanto impacto secuestrando cientos de miles de dispositivos alrededor de todo el mundo. La investigación de Sophos revelo que el ataque de WannaCry se produjo en 3 etapas, ejecución de código malicioso para obtener privilegios de usuario avanzados. Luego el código del malware fue ejecutado para hacer el cifrado de documentos y mostrar las notas de rescate.

Los atacantes usaron un código filtrado por un grupo de hackers conocidos como shadow Brokers el cual aprovechaba la falla de Microsoft para propagar el gusano que dejo caer WannaCry en los pc de todo el mundo. Estando allí WannaCry uso cifrado en archivos como documentos, videos e imágenes. Con las herramientas de explotación filtradas por personas como shadow Brokers se espera que se sigan presentando este tipo de ataques durante 2018.

Estadisticas de Amenaza

Mcafee labs report es un reporte que la compañía de seguridad informativa McAfee, publica cada trimestre, en este se muestran investigaciones y estadisticas realizadas por el equipo de Investigacion de Amenzas de la compañía. Durante el primer trimestre del año 2018 se publico la tendencia en la disminucion de nuevas Muestras de Ransomware ,es decir nuevas variantes que tienen el comportamiento de este tipo de malware. Mientras que el numero de muestras ya existentes aumento de manera significativa, aumentando

en un 62 % en los últimos cuatro trimestres. En la figura 10 se observa la el crecimiento de variantes actuales y aquellas que ya eran conocidas.

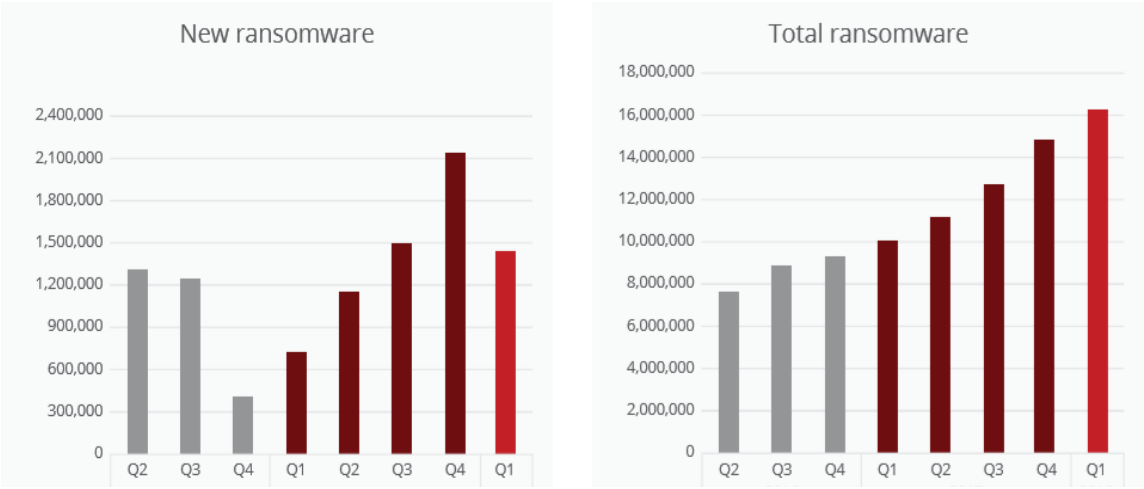

Figura 10. Variantes de Ransomware primer trimestre 2018. Fuente "Threats Report McAfee Labs June 2018"

La Figura 11 muestra un crecimiento que ha tenido Ransomware, desde sus inicios.

Figura 11. Línea de tiempo Ransomware. Fuente https://www.tcdi.com/Ransomware-timeline/

2.4.5. AVANCES PARA PROTECCIÓN DE AMENAZAS CRYPTO RANSOMWARE

Una de las principales actividades para hacer frente y mejorar la seguridad sobre amenazas informáticas, consiste en mejorar la visibilidad de los eventos de seguridad, también hacer uso de la correlación de eventos y en la automatización de procesos para dar respuesta a incidentes. Este tipo de procesos requieren de tecnológicas que puedan comunicarse e interactuar entre sí, que hagan intercambio de información y usen herramientas de aprendizaje automático para la toma de decisiones.

“Es muy importante también tener programas de educación y divulgación de seguridad respecto a vulnerabilidades, amenazas, políticas y procedimientos. Las personas suelen ser vulnerables a diversos ataques y pueden ser grandes aliadas si están comprometidas con la seguridad. Un punto que no se debe olvidar es incorporar a la cadena de proveedores en nuestros procesos de seguridad” (Cruz, 2017).

Algunos expertos en seguridad manifiestan: “Los productos tradicionales de seguridad de Endpoint se han movido más allá de los antivirus y los cortafuegos personales, y más productos se han centrado en cerrar la brecha entre la detección y respuesta de punto final. Este cambio refleja la creciente necesidad de identificar y remediar las amenazas en menos tiempo” (Techtarget, 2016). Una nueva amenaza obliga a que los profesionales y compañías de software y hardware en seguridad se esfuercen mediante sus investigaciones y pruebas de laboratorio de manera rápida para lograr encontrar la forma de blindarse frente a cada evolución de malware; aunque no es lo único que resta por hacer, pues una directriz actual afirma que también es necesario y altamente importante que los analistas de seguridad de la información estén siempre bien entrenados y aumenten su conocimiento constantemente; esta es la solución más efectiva contra las amenazas persistentes avanzadas. Dichas personas, líderes en el área de tecnologías de la información en las compañías, deberían procurar porque se le dé la importancia que merece la protección de los datos y se destinen esfuerzos para mantener y mejorar esa seguridad, pues ser víctima de un ataque podría ocasionar serios e irreparables daños.

Las compañías desarrolladoras de sistemas Endpoint están en la búsqueda de soluciones con más cobertura, es decir, que protejan tanto sus equipos de escritorio y portátiles

como sus dispositivos móviles, y así poder brindar métodos que proporcionen un entorno más seguro. A pesar de los cambios constantes que se han generado por parte de las casas de software, éstos no han podido cubrir todas las necesidades que se han generado en los últimos años. La evolución constante de este tipo de amenazas genera una incesante búsqueda de métodos y estrategias que permitan evitar ser afectados por infecciones.

2.5. SEGURIDAD ENDPOINT

Se refiere al proceso de asegurar los distintos dispositivos finales que se encuentran en una red corporativa; estos dispositivos pueden ser computadores, servidores, equipos móviles, entre otros.

Cualquier dispositivo que tenga acceso a la red, es un punto de entrada para amenazas que intenten vulnerar la seguridad del entorno corporativo; de allí que el perímetro que antes protegía la red interna de intrusiones ha disminuido su protección. Este tipo de seguridad está diseñado para proteger la red y bloquear cualquier intento de amenaza en estos dispositivos.

Un Endpoint es un dispositivo de hardware de computadora, compatible con Internet en una red TCP/IP. “El término se refiere a los Computadores de escritorio, Equipos portátiles, Smartphone, Tabletas, y otro hardware que cumpla funciones de cómputo en una red de datos” (Rouse, Techtarget, 2013). En la figura 12 se puede visualizar algunos de los dispositivos de usuario final.

Figura 12. Esquema de red. Fuente http://www.asigra.com/sites/default/files/images/logos/diagram-endpoint-devices.png

Las soluciones de seguridad Endpoint consisten en un sistema de seguridad que se ubica de manera centralizada en un servidor, y agentes que se despliegan en cada uno de los dispositivos que hacen parte de la red corporativa. Desde el servidor que hace las veces de consola de administración se realizan actualizaciones de firmas de antivirus, se despliegan políticas generales, según las necesidades que tenga el personal de seguridad, y también autentica los inicios de sesión de los equipos para otorgar derechos a los dispositivos de usar los recursos de la red.

Los software antivirus tienen funciones básicas de protección con bases de datos de firmas de malware, mientras que las consolas de seguridad Endpoint cuentan con características adicionales para la seguridad, entre las cuales se encuentran data loss Prevention, que se encarga de la protección de fuga de datos en un entorno controlado; firewall, para controlar los puertos que utiliza el dispositivo; HIPS, para proteger el equipo ante intrusiones. Estas y otras funcionalidades hacen que la seguridad Endpoint esté a la vanguardia de la protección de dispositivos en una red.

2.6. SEGURIDAD PERIMETRAL INFORMÁTICA

Se refiere a un grupo de elementos informáticos integrados, destinados a la protección del perímetro de una red interna frente a otra, que generalmente es internet. Algunas de sus características son las siguientes:

- Detección de intrusos.
- Denegación de accesos no autorizados.
- Equipos UTM de borde.
- Acceso a usuarios internos y externos.
- Audición al tráfico entrante y saliente.
- Definición de niveles de confianza.

La seguridad perimetral cuenta con una serie de elementos, que se describen a continuación:

2.6.1. FIREWALL

El firewall es un sistema de seguridad de red que permite filtrar los paquetes de datos que viajan a través de internet, en tráfico entrante y saliente. Pueden ser soluciones de hardware o de software; designado para permitir o denegar el acceso a los datos de la red local a usuarios de otras redes.

La tarea del firewall es revisar cada bit que intenta ingresar o egresar de nuestra red, aplicarle una lógica de comparación (obtenida de la configuración de políticas de seguridad en el mismo firewall) y, según los resultados, permitir o denegar el paso de dicha información hacia la red destino. Sobre la base de este comportamiento, existen dos premisas principales:

1. **Restrictiva:** todo lo que no esté explícitamente permitido, será restringido.
2. **Permisiva:** todo lo que no esté explícitamente restringido, será permitido.

"El firewall basará su proceso de decisión en la premisa que haya sido seleccionada en su política de configuración, y continuará realizando las comparaciones necesarias para determinar si permite el tránsito de la información, o lo bloquea" (Garcia, 2014).
El firewall se encarga de filtrar los paquetes por protocolo, puerto de conexión u origen y destino. Cualquier tipo de dato que no esté permitido es bloqueado, y el firewall impide su ingreso a la red.

Este tipo de firewall trabaja principalmente en las capas de transporte y red del modelo OSI. La capa de transporte es la encargada de identificar el puerto origen y destino, de manera eficiente; pero ésta no es capaz de identificar si el tráfico hace parte de los datos confiables.

Por actuar bajo la capa de aplicación del modelo OSI; el modo de operación de este tipo de firewall es más complejo que solo el filtrado de paquetes, pues debe conocer cada uno de los protocolos con los que trabajan las aplicaciones. Puede identificar si un protocolo está siendo usado a través de un puerto poco común, y si su uso es para la afectación de la red, lo que hace a este firewall efectivo, y permite obtener una protección de la red.

2.6.2. UTM

Es conocida como gestión unificada de amenazas; es un único producto de seguridad que cuenta con varias características de productos que generalmente se ofrecen de manera individual; algunas de sus funciones son:

- Prevención y detección de intrusiones en la red centrada en el bloqueo de ataques contra PC y servidores (IDS/IPS).
- Detección y bloqueo de antivirus y antimalware
- Filtrado antispam
- Filtrado del contenido web y URL
- Funciones habituales de firewall (cortafuegos)
- Acceso remoto site-to-site (de sitio a sitio), con soporte en VPN y SSL (basado en navegador).

El UTM permite al administrador desde una única consola, administrar y monitorear los aspectos de seguridad relacionados con el perímetro

2.6.3. IDS (INTRUSION DETECTION SYSTEM)

Son sistemas que trabajan en conjunto con el Firewall, brindando un nivel de seguridad mayor. Su función principal es generar información de eventos dudosos o anormales por medio del reconocimiento y envió de logs. Estos sistemas trabajan para detectar intrusos en su área de cobertura, mediante alertas tempranas enviadas a administradores.

Sus funciones principales son:

- Identificación de posibles ataques
- Registro de eventos
- Reporte al administrador de posibles ataques

Clasificación:

- NIDS (Network Based IDS). Controla el tráfico en busca de actividades sospechosas.

- HIDS (Host Based IDS). Protege a un solo equipo; monitoriza cambios en el sistema operativo y aplicaciones.

Modos de detección

Detección basada en firmas: son modelos que se refieren a cómo los ataques son realizados y cómo pueden ser detenidos. Cualquier acción que no sea reconocida como un ataque será considerada como aceptable; es decir, este tipo de detección es débil contra nuevos ataques.

Detección basada en patrones de comportamiento: se observa y detecta variaciones del comportamiento esperado por parte de los usuarios y los sistemas; detecta nuevas y desconocidas vulnerabilidades; sin embargo, puede causar muchas falsas alarmas. En la figura 13 y 14 se observa una de las configuraciones comunes de un IDS y IPS respectivamente.

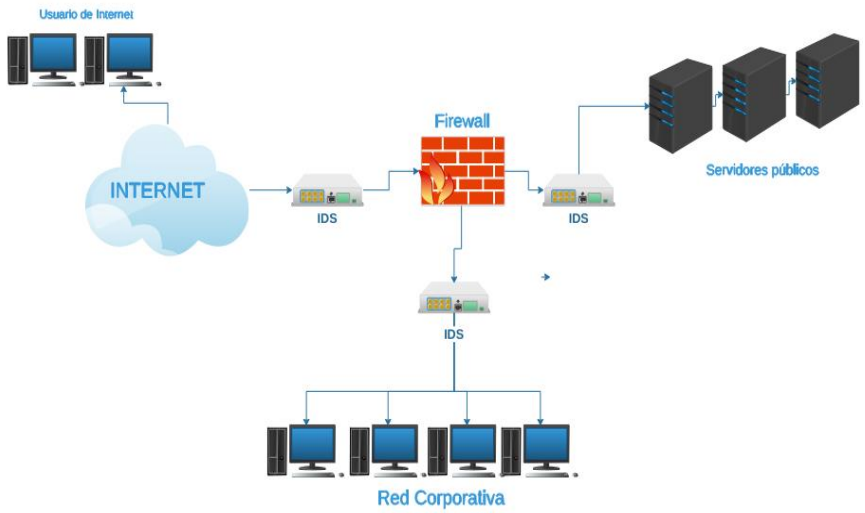

Figura 13. Diagrama IDS. Fuente Autores.

2.6.4.IPS (INTRUSION PREVENTION SYSTEM)

Trabajan en la misma forma que los IDS, pero con la diferencia de permitir el análisis de la información en tiempo real. Estos equipos poseen una puerta de entrada y salida. Al momento de recibir información por un extremo de conexión, se la analiza inmediatamente, en búsqueda de potenciales ataques o intrusiones. Si la información es aprobada, el paquete es transmitido al otro extremo de la conexión; en caso contrario, el IPS podría reaccionar de manera preventiva, logrando que ni siquiera un paquete malicioso sea incorporado en la red o el equipo bajo su protección.

Métodos de detección

- Detección basada en firmas.
- Detección basada en políticas.
- Detección basada en anomalías.

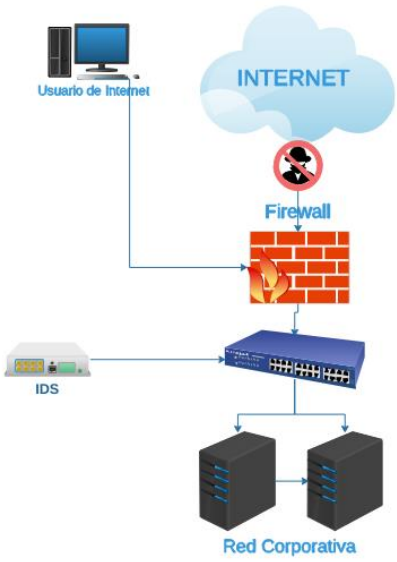

Figura 14. Diagrama IPS. Fuente Autores.

2.7. COPIAS DE SEGURIDAD

Existen diferentes motivos por los cuales la información que se encuentra almacenada en equipos o servidores puede sufrir daños o perderse de forma permanente, entre los que se encuentran Malware, fallas en el hardware, usuario con la intención de hacer daños, accidentes o descuidos.

Los backup o copias de seguridad, son copias de los datos que contienen un sistema realizadas para que puedan ser recuperadas en caso de fallo, borrado accidental o cualquier otra contingencia. (Ramos, 2011).
Estos datos pueden ser almacenados en medios extraíbles, tales como:

- Cintas magnéticas
- USB
- CD
- DVD
- Ubicaciones de red
- Cloud
- Discos Duros

Realizar copias de seguridad de manera periódica es importante para mantener los respaldos actualizados; éstas se realizan de los datos que componen el sistema, o de archivos específicos que utiliza el usuario en su día a día.

Los backup componen la última línea de defensa frente a amenazas que pongan en peligro la información, y son el último recurso que se utiliza. Existen diferentes modelos de almacenamiento, según como sean almacenadas las copias de seguridad.

2.7.1. MODELOS DE ALMACENAMIENTO DE DATOS

Desestructurado: son discos que contienen la información de la copia de seguridad, pero no conservan una estructura que tenga la información de cuándo y a qué se le realizó la copia de seguridad para su posterior recuperación.

Incremental: es un modelo que consiste en realizar varias copias de seguridad de la información**.** Se realiza una primera copia de seguridad completa de la fuente de datos, luego se continúa con copias de seguridad incrementales que consiste en tomar solamente los datos que han sido modificados desde la última copia de seguridad completa. Para realizar una restauración con este modelo se necesitaría la copia de seguridad completa y cada una de sus incrementales para la restauración óptima.

Diferencial: este modelo copia los archivos que han sido modificados desde la última copia de seguridad completa; se necesita más espacio que las copias incrementales, pero, a la hora de realizar una restauración, simplemente se necesitaría la copia de seguridad completa y la última copia de seguridad diferencial.

2.7.2. SERVIDOR DE ARCHIVOS

Es un equipo configurado, con el fin de almacenar y gestionar la administración de datos en una organización; el modelo que utiliza para este servicio se basa en cliente/servidor. Cuando los usuarios de la red necesiten un archivo, podrán acceder a éste a través del servidor de archivos, sin necesidad de pasarlo manualmente por medios extraíbles. Existen diferentes protocolos utilizados por servidores de archivos para la transferencia de archivos entre clientes y servidores.

El protocolo del Bloque de mensajes del servidor (SMB) es un protocolo de uso compartido de archivos de red, que permite que los programas de un equipo puedan leer

y escribir archivos y solicitar servicios desde los programas de un servidor en una red de equipos windows y linux.

CIFS (Common Internet File System) es un protocolo de red que proporciona la capacidad del uso compartido de archivos, basado en Windows y otras utilidades de red.

NFS (sistema de archivos de red: Network File System) es un protocolo que permite acceder a un sistema de archivos, a través de la red. Es compatible con sistemas que utilicen Unix.

2.7.3. COPIA DE SEGURIDAD DE UN SERVIDOR DE ARCHIVOS

A continuación, se describe el proceso básico de realización de copia de seguridad a un servidor de archivos, utilizando una herramienta llamada acronis backup; es una herramienta de un proveedor de servicios de respaldo de información que tiene la posibilidad de hacer copias de seguridad tanto de sistemas operativos windows, como Linux.

Es un servicio que corre directamente desde la nube, por lo cual no requiere la instalación de un servidor para la consola de administración.

1. Se ingresa a la consola de administración del servicio; allí se selecciona cuál sistema operativo se desea respaldar; en este caso será un servidor de archivos windows.

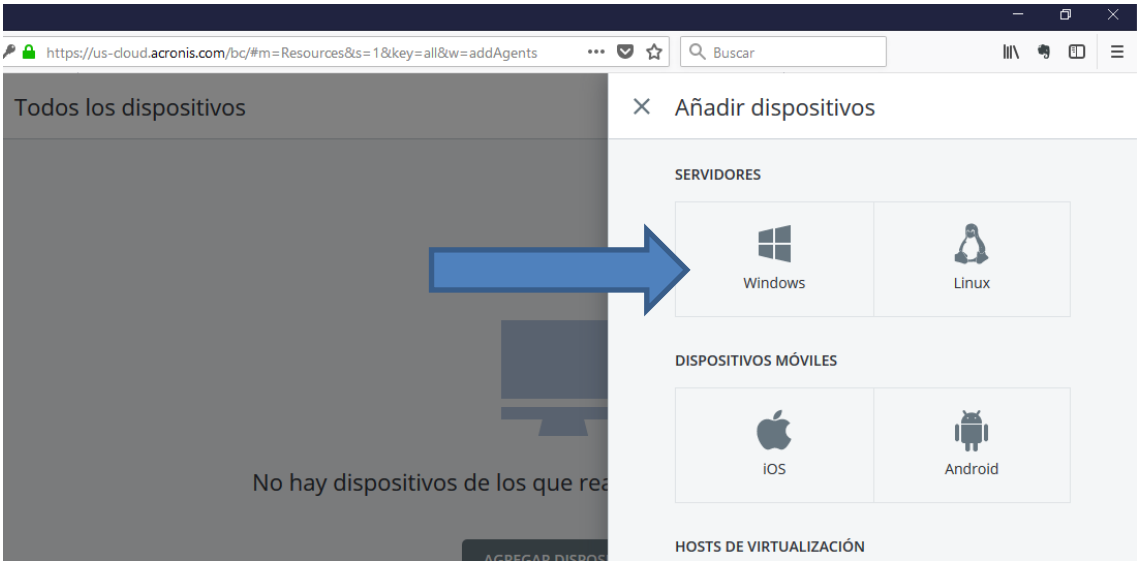

Figura 15. Herramienta de backup acronis backup cloud. Fuente Autores.

2. Se descarga un archivo ejecutable en el servidor; este se debe instalar. A continuación, aparecerá el servidor gestionado en la consola de administración principal.

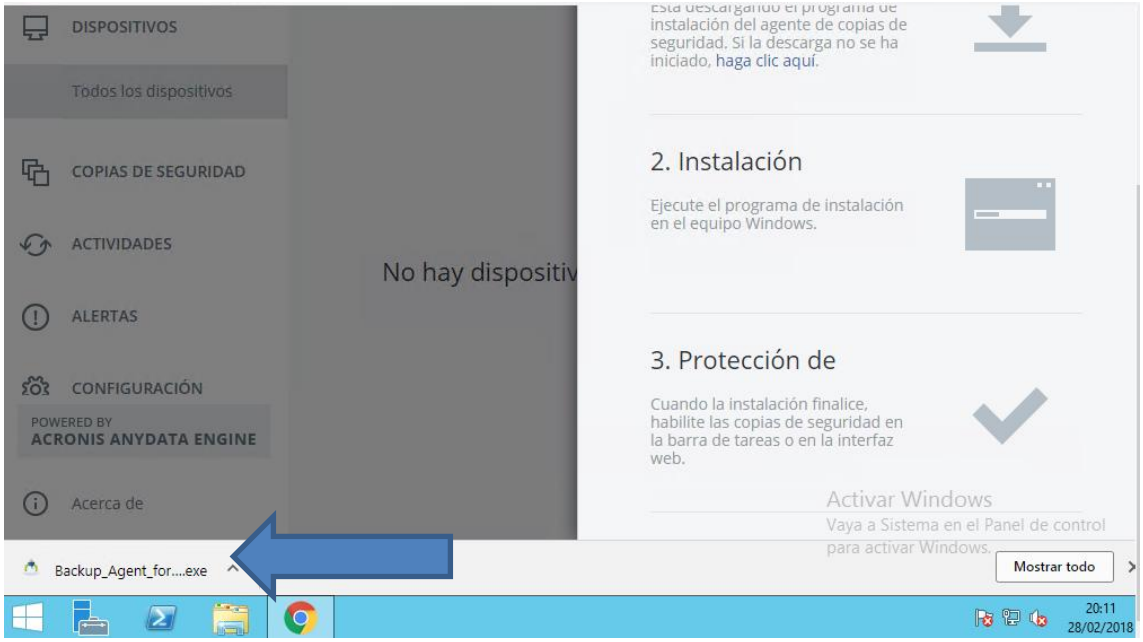

Figura 16. Instalación de agente en servidor. Fuente Autores.

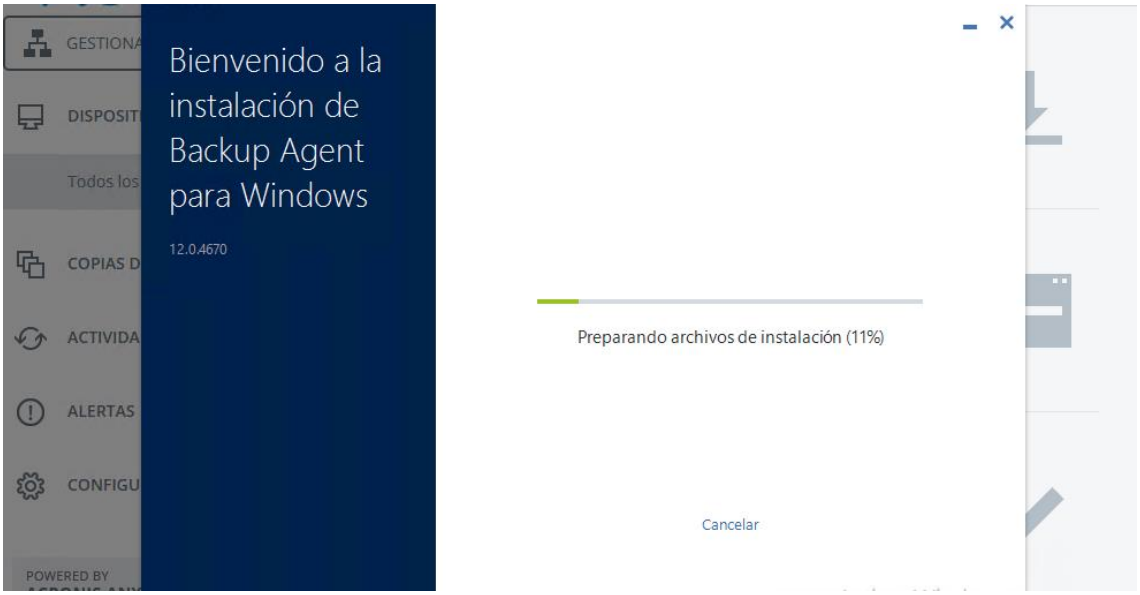

Figura 17. Ejecución e inicio de instalación de agente. Fuente Autores.

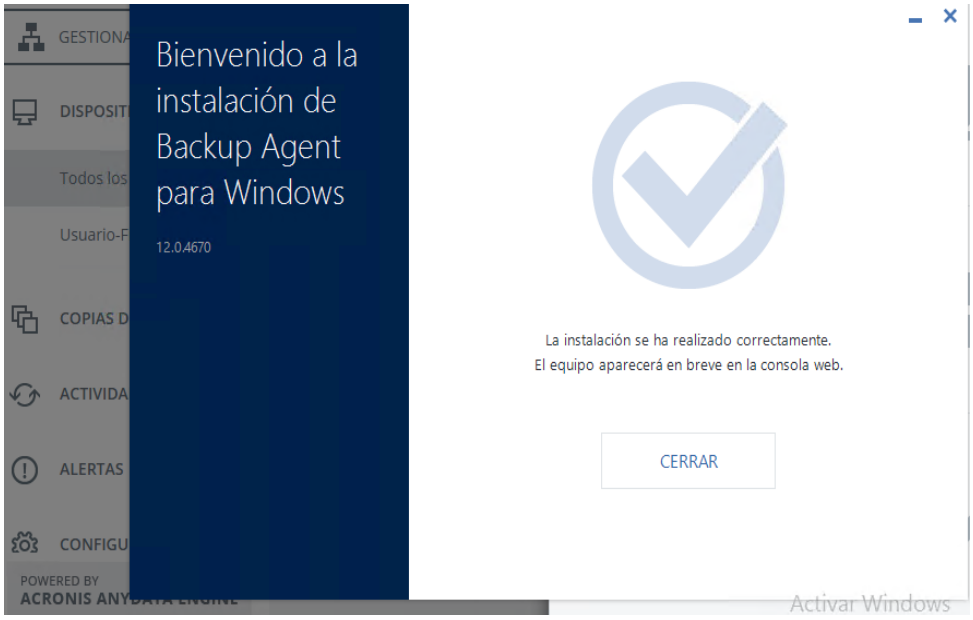

Figura 18. Finalización del proceso de instalación. Fuente Autores.

3. Una vez se realiza la instalación del agente en el servidor, se verifica que este ya se encuentra gestionado en la consola de administración principal.

Figura 19. El servidor está gestionado en la consola principal. Fuente Autores.

4. Luego se selecciona la opción de copia de seguridad; allí hay una serie de parámetros que deben ser configurados.

- Qué incorporar en la copia de seguridad: allí se selecciona el equipo completo para poder realizar una recuperación de todo el equipo
- Dónde se guardará la copia de seguridad; allí se selecciona una ruta de red, que apunta a una NAS de almacenamiento, y allí se guardarán los datos de la copia de seguridad.
- Planificación: acá se define la frecuencia del backup; se puede escoger una copia de seguridad incremental de lunes a viernes. Esto, con el fin de sólo copiar los datos que han cambiado desde la última copia. El fin de semana se puede realizar una copia de seguridad completa que sería una copia más extensa.

- Cuánto tiempo se conservará: allí se define la retención de las copias de seguridad, por defecto está definida en 6 meses, pero se puede modificar, en caso de requerir conservar las copias más tiempo.
- Cifrado: el cifrado de la copia de seguridad se configura con el fin de proteger la confidencialidad de la información que contiene la copia de seguridad.

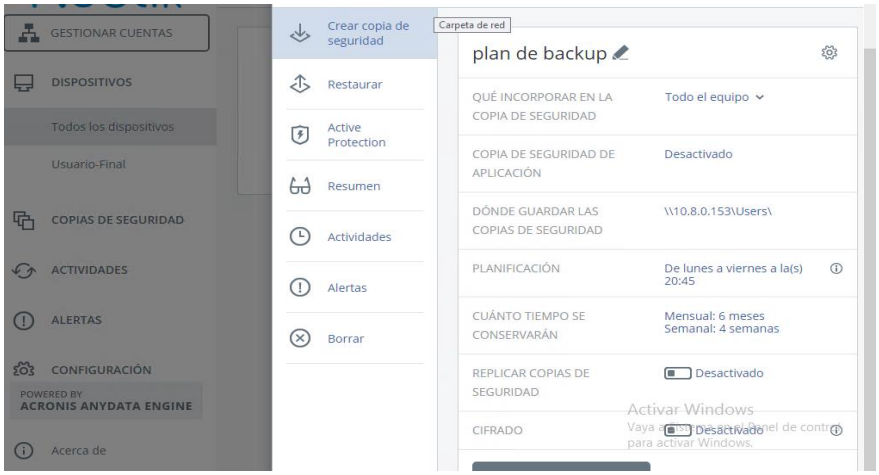

Figura 20. Configuración de parámetros de la copia de seguridad. Fuente Autores.

5. Se puede iniciar la copia de seguridad de inmediato, o ésta también iniciará según la programación. La consola principal indicara los puntos de restauración existentes almacenados en la NAS de almacenamiento.

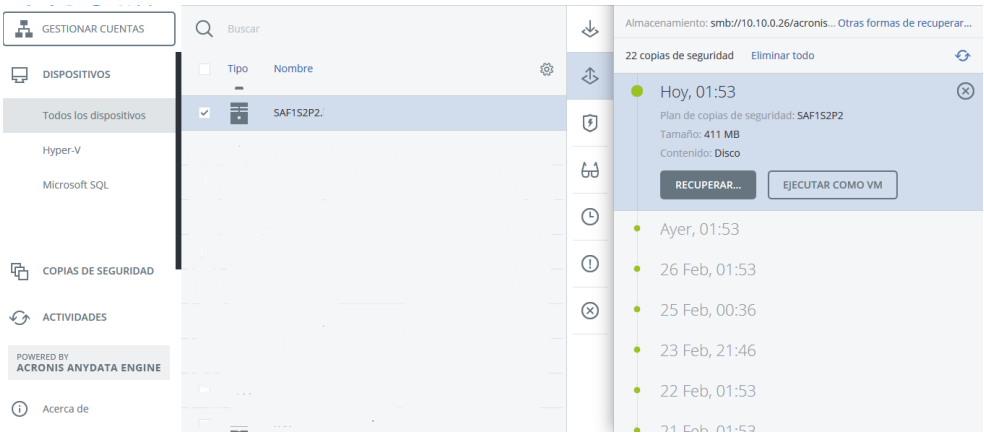

Figura 21. Puntos de restauración almacenados. Fuente Autores.

2.8. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

Son documentos o sugerencias de seguridad, diseñados para las empresas o entidades, como un plan de prevención y acción que permiten determinar el alcance de la necesidad de la seguridad para cada compañía y define los activos que requieren ser protegidos. Dichas políticas deben mostrar los requerimientos de cada organización; además, identificar las áreas fundamentales y el motivo por el que cual se deben proteger.

Las políticas de seguridad de la información son clasificadas de la siguiente manera:

Políticas de regulación: se usa cuando los estándares legales se puedan aplicar a la empresa. Son mandatorios y contienen la descripción de cada uno de los procedimientos que se deben ejecutar para ser cumplidas.

Políticas de consejo: este tipo de políticas se usa para definir el tipo de comportamientos y actividades que son aceptadas y, adicionalmente, son definidas las consecuencias cuando se comenten violaciones.

Políticas de información: su fin es el de brindar información acerca de datos muy específicos de cada compañía, como los valores corporativos, misión, visión, datos de clientes y proveedores, entre otros.

2.8.1. ESTÁNDAR ISO/IEC 27001:2013

Es una norma internacional expuesta por la Organización Internacional de Normalización (ISO), la que se define cómo debe ser gestionada la seguridad de la información en una organización. La primera publicación se dio en 2005, y en 2013 se realizaron las modificaciones más recientes. Estas modificaciones reciben el nombre de ISO/IEC 27001:2013. Esta es una norma que ayuda a las organizaciones a gestionar la seguridad de los activos que posea.

Está es una norma a nivel mundial para la seguridad informática; las compañías, cada vez con más frecuencia, buscan certificarse, lo que define que la organización certificada tiene políticas de seguridad implantadas en cumplimiento de la ISO 27001.

El estándar ISO/IEC 27001:2013 presenta un Anexo A, que toma los controles de seguridad de la ISO/IEC 27002:2013, donde se presentan los Dominios (14), Objetivos de Control (35) y Controles de Referencia (113).

Anexo A ISO27001:2013 Objetivos de Control	
A.5	Políticas de seguridad
A.6	Organización de la información
A.7	Seguridad en recursos humanos
A.8	Gestión de activos
A.9	Control de accesos
A.10	Criptografía
A.11	Seguridad física y ambiental
A.12	Seguridad en las operaciones
A.13	Transferencia de la información
A.14	Adquisición de sistemas, desarrollo y mantenimiento
A.15	Relación con proveedores
A.16	Gestión de los incidentes de seguridad
A.17	Continuidad de negocio
A.18	Cumplimiento con requerimientos legales y contractuales

Tabla 3. Objetivos de control ISO27001:2013. Fuente http://www.iso27000.es/download/ControlesISO27002-2013.pdf

ANEXO A.17 CONTINUIDAD DE NEGOCIO

En los planes de la continuidad de negocio se pretende mantener la seguridad de la información en todas las fases del proceso, tales como la activación y el desarrollo de procesos y procedimientos.

En el momento de incorporar y evaluar procesos críticos de las organizaciones, se debe incluir aquellos en los que se vean involucrados la gestión de la seguridad de la información en la legislación, los recursos, la legislación, entre otros.

Se debe considerar la causa de los inconvenientes de seguridad, pérdidas y disponibilidad de servicios; además, tener en cuenta la implementación de planes de contingencia que permitan que los procesos de cada organización se puedan restablecer dentro de los tiempos de gestión requeridos para las operaciones fundamentales, conservando las previsiones de seguridad de la información usada en los planes de continuidad y función de los resultados del análisis de riesgos.

Es necesario, de manera continua realizar pruebas como simulacros, benchmark, etc., que permitan mantener los planes actualizados, aumentando la confianza, y darlos a conocer a cada uno de los empleados involucrados.

17.1 Continuidad de la seguridad de la información

El objetivo es sostener la seguridad de la información en integración con los sistemas de gestión de continuidad de negocio en cada organización.

17.1.1 Planificación de la continuidad de la seguridad de la información. Es de vital importancia que las compañías, ante situaciones desfavorables, tengan definidas las exigencias para la seguridad de la información y su gestión.

17.1.2 Implantación de la continuidad de la seguridad de la información. Las organizaciones deben tener establecidos, documentados e implementados, los procesos, procedimientos y controles para certificar el sostenimiento del nivel necesario de seguridad de la información durante situaciones desfavorables.

17.1.2 Implantación de la continuidad de la seguridad de la información. Las organizaciones deben tener establecidos, documentados e implementados, los procesos, procedimientos y controles para certificar el sostenimiento del nivel necesario de seguridad de la información durante situaciones desfavorables.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. Las organizaciones deberán confirmar los controles de continuidad de la seguridad de la información determinados e implementados, para poder probar su validez y eficacia ante situaciones desfavorables.

17.2 Redundancia

La redundancia se conoce como alta disponibilidad, debido a que involucrase la capacidad de que cualquier sistema descubrir una falla de manera eficaz y restablecer el servicio en el menor tiempo posible. Además, se entiende como en proceso en el que dos sistemas completos están replicados.

El objetivo es proporcionar y certificar la disponibilidad de las instalaciones de procesamiento y almacenamiento de la información.

Se pueden encontrar una variedad de tipos de redundancia que comprende diferentes componentes o sistemas en una compañía. Entre estos encontramos; De red, en esta parte comprende que se tiene un respaldo de proveedor de internet en el momento que el principal tenga inconvenientes. De hardware, se entiende por los componentes y equipos físicos para actuar ante una emergencia. De sistemas eléctricos, estos permiten que los servidores continúen en operación después de una falla eléctrica por lo que se usan UPS, manteniendo el datacenter encendido por un tiempo determinado.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. Es necesario realizar la implementación de la redundancia necesaria en las instalaciones de procesamiento de la información, que respondan con las exigencias de disponibilidad.

2.8.2. FRAMEWORK DE LA NIST SP 800

Es un marco de referencia para el mejoramiento de la seguridad de la información. Fue publicado en el año 2014 por el US National Institute of Standards and Technology (NIST). Su función es la de evaluar y mejorar la capacidad de las organizaciones para prevenir, detectar y responder a los ataques cibernéticos. Está siendo utilizado por una amplia gama de empresas y organizaciones, y la ayuda a ser proactivas sobre gestión del riesgo.

"La serie NIST 800 es un conjunto de documentos que describen las políticas, procedimientos y directrices de seguridad informática del gobierno federal de los Estados Unidos. NIST (Instituto Nacional de estándares y tecnología) es una unidad del Departamento de comercio. Los documentos están disponibles gratuitamente y pueden ser útiles a las empresas y a las instituciones educativas, así como a las agencias gubernamentales".**Fuente especificada no válida.**

Una organización puede utilizar el marco como parte clave de su proceso sistemático para identificar, evaluar y administrar el riesgo de ciberseguridad. El marco no está diseñado

para sustituir los procesos existentes; una organización puede utilizar su proceso actual y superponerlo en el marco para determinar las brechas en su enfoque actual de riesgo de ciberseguridad, y desarrollar una hoja de ruta para mejorar. (Technology, 2014)

2.8.3. COBIT (Control Objectives for Information and related Technology)

Es un marco de referencia utilizado y aceptado internacionalmente como buenas prácticas en las implementaciones de tecnologías de la información, controles del riesgo y seguridad de la información. El propósito de Cobit es brindar a la gerencia de una compañía confianza en los sistemas de información y en la información que éstos produzcan. Cobit permite entender cómo dirigir y gestionar el uso de tales sistemas, así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas. Cobit suministra las herramientas para supervisar todas las actividades relacionadas con IT.

Algunas de las ventajas de implementar Cobit:

i. Los departamentos de sistemas de información entregarán resultados de manera más oportuna y de mejor calidad
ii. Los procesos de calidad serán más eficientes, y de igual manera su administración
iii. Las gestiones de riesgos en la organización serán realizadas con mayor efectividad
iv. Utilizar un lenguaje común para que los administradores puedan comunicar sus resultados.

3. METODOLOGÍA

El proyecto consta de 3 fases, las cuales se detallan a continuación:

Dictamen de los objetivos del proyecto y definición del alcance

Se inició con una evaluación del estado actual de la amenaza Crypto Ransomware, y así se definieron los objetivos que buscan brindar seguridad de la información a las PYMES. Además de la definición de políticas y procedimientos de protección, se definió un plan de copias de seguridad en un servidor de archivos con su respectivo plan de recuperación, y finalmente, se generó un mapeo de políticas y procedimientos basados en la norma ISO27001:2013.

Recopilación de la información

En esta etapa se realizó levantamiento de información para construir el marco teórico; se recopilaron datos sobre investigaciones, publicaciones y artículos a cerca de amenazas Crypto Ransomware y elementos de seguridad informática. Fueron usados libros de seguridad, consultas de blogs de empresas de seguridad con enfoque en desarrollo de productos y servicios de seguridad informática; también se tomaron artículos sobre el estado actual de las amenazas Ransomware.

Desarrollo de las mejores prácticas

Es esta fase del proyecto fueron tomadas las fuentes de información consultadas y se procedió con la construcción de las políticas y procedimientos de seguridad para PYMES, que agregarán una capa de seguridad ante Crypto Ransomware, junto a la elaboración de

un plan detallado de copias de seguridad en servidores de archivos y el mapeo, basados en la norma ISO27001/2013 que contiene el Anexo A, que consta de una serie de controles, de los cuales usamos la continuidad de negocio. A continuación, se describen las políticas diseñadas tanto a nivel perimetral como a nivel de dispositivos de usuario final; también se propone un plan de recuperación frente a una pérdida de integridad de los datos en un servidor de archivos.

3.1 POLÍTICAS PARA PROTECCIÓN A NIVEL PERIMETRAL FRENTE AL RANSOMWARE

Los dispositivos de seguridad para poder brindar un nivel de protección adecuado deben ir acompañados de una serie de políticas en sus configuraciones, que permiten un nivel óptimo de protección; es decir, no basta con adquirirlos o comprar su licencia; este debe ir configurado de tal forma que proteja de manera adecuada. El diseño de las siguientes políticas fueron realizadas en base a documentos de empresas de seguridad informática y artículos de expertos en TI y pueden ser aplicadas en dispositivos de protección perimetral.

El esquema de red está basado en 2 elementos: los componentes básicos que componen una red LAN (Rouse, techtarget, 2016) como dispositivos de red, equipos y servidores. Adicionalmente se agregó un dispositivo de seguridad perimetral que protegerá esta red LAN de su interacción con una red pública como lo es internet. En el esquema se utiliza un dispositivo UTM, ya que este se compone de varios módulos de otros dispositivos perimetrales, tales como firewall, IPS, proxys, entre otros. De esta forma, las políticas mencionadas a continuación podrán ser aplicadas tanto a UTM como a otros dispositivos de la misma clase.

Basados en un marco de referencia como NIST (Technology, 2014) que permite gestionar de una manera más esquematizada la seguridad de la red, se propone una serie de políticas que pueden ser aplicadas a pequeñas empresas, en busca de tener una primera

capa de protección frente a amenazas de tipo Crypto Ransomware; también se tienen en cuenta buenas prácticas aceptadas por las mejores empresas de seguridad del sector, tales como McAfee y Trend micro (Trend Micro, 2017). Estas políticas también son orientadas al tipo de amenaza ya mencionado.

- **ESQUEMA DE RED**

  Esquema de red básico donde se encuentran dispositivos de red, dispositivos Endpoint y dispositivo de seguridad de perímetro, se puede ver gráficamente la red interna separada de la red externa por un dispositivo firewall perimetral.

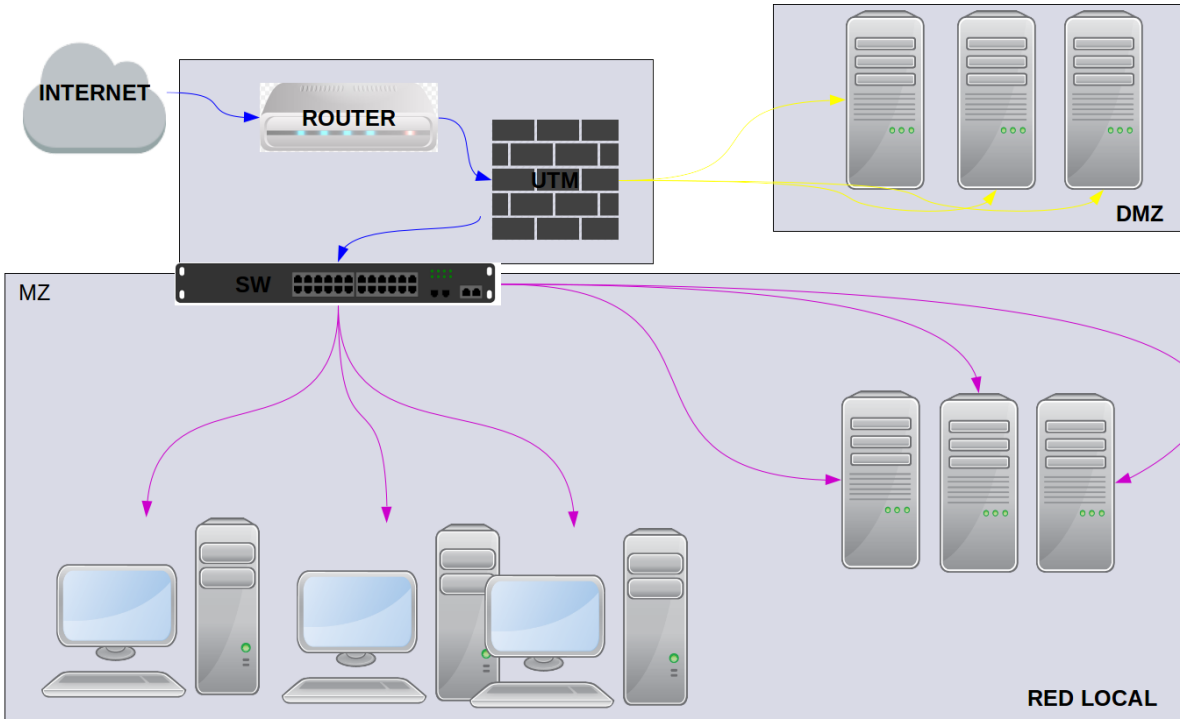

Figura 22. Esquema de red con UTM. Fuente Autores

POLÍTICAS SEGURIDAD PERIMETRAL

IDENTIFICAR

- ***Definir políticas de usuarios con acceso a la administración.***

Se deben tener definidas y documentadas las personas que van a tener derechos administrativos de los sistemas y servicios en la organización, es decir, aquellos usuarios administradores de TI que manejarán cuentas de súper usuario o usuarios con nivel de privilegios elevados, los cuales podrán realizar cambios significativos o parciales en los equipos; estos cambios realizados deben tener una documentación completa en la que se detalle la causa, el diagnóstico y procedimiento que se siguió al realizar el cambio.

- ✓ En vez de que todas las personas que ingresen a los dispositivos de seguridad accedan con la cuenta administrador por defecto, se debe crear una cuenta para cada persona, con su nombre y asignar los permisos necesarios.
- ✓ Los dispositivos de seguridad vienen por defecto con una cuenta de administrador o admin. Para un atacante sería mucho más fácil realizar un ataque dado que sólo necesitaría la contraseña. Se recomienda cambiar el nombre de la cuenta administrador por uno diferente de más difícil acceso
- ✓ Cuando sea necesario la administración remota, es importante habilitar el acceso, solo desde algunos dispositivos seguros que se configuran previamente, para que, de esta forma, no se pueda acceder desde cualquier lugar
- ✓ Modificar el puerto de ingreso que viene por defecto es una buena práctica para que a los posibles intrusos les sea más complicada la tarea de acceso al dispositivo.
- ✓ Para evitar la posibilidad de que un administrador pueda dejar su sesión iniciada en un dispositivo del cual se haya movido, se debe configurar un tiempo máximo de sesión, en el cual la persona deberá volver a iniciar sesión para continuar su trabajo.
- ✓ Habilitar una política de contraseña; esto evitará que un usuario pueda colocar una contraseña que sea de fácil acceso para un atacante; la contraseña deberá tener una longitud mínima, contener letras mayúsculas y minúsculas y también agregar caracteres especiales.

PROTEGER

- ***Actualizar el software de su dispositivo de seguridad Perimetral, herramienta de antivirus o firmas IPS a la versión más reciente***.

Cuando se crea software por parte de los fabricantes, aquellos no son infalibles, y pueden tener vulnerabilidades en su código que, en ocasiones, son descubiertas y aprovechadas por ciberdelincuentes para su beneficio personal. Estos fabricantes, al descubrir tales fallas en el código, realizan ciertas revisiones y publican parches de seguridad para salvaguardar su software. El problema se genera cuando el usuario no realiza actualizaciones a tiempo; esto da pie a que el ciberdelincuente siga aprovechando esta ventaja, para él.

- ***Activar el filtrado WEB***

Muchos de los servidores que alojan el malware y también los servidores de comando y control se alojan en dominios de procedencia maliciosa; es por esto de vital importancia restringir la navegación a los empleados de la organización a este tipo de dominios.

Tareas a tener en cuenta en la puesta en marcha del filtro Web.

- ✓ Siempre tener habilitado el filtrado web. Esto ayudará a prevenir infecciones de malware y, en caso de infección, comunicar a servidores maliciosos.
- ✓ Bloquear categorías como pornografía, malware, phishing, Spyware. Son categorías propensas a contener peligros informáticos

- ***Activar el Firewall de red***

Crear reglas de listas blancas o listas negras, donde se permita todo el tráfico, y bloquear aquel que no se desee o, por el contrario, restringir todo, y sólo habilitar los puertos que son necesarios para el trabajo de la organización.

Tareas a tener en cuenta en la puesta en marcha del Firewall:

- ✓ Al configurar o eliminar una configuración del firewall, éste tomará efecto de inmediato sobre la red.

- ✓ Organizar las políticas de firewall, de la más específica a las más general; es decir, la política con un mayor número de direcciones de red coincidentes será una política más general.
- ✓ Asignar nombres a las interfaces del dispositivo mejora su administración y configuración.
- ✓ Evitar usar la selección. Todos para las direcciones de origen y destino. Use direcciones o grupos de direcciones.

- ***Usar filtros ANTISPAM***

El medio más utilizado para la propagación del Ransomware son las campañas de spam. A través de correos electrónicos se envían links o archivos comprimidos que contiene el medio para la infección.

Tareas a tener en cuenta en la puesta en marcha del filtro Antispam.

- ✓ Usar un perfil de seguridad específico para la regla antispam

- ***Usar Filtros IPS***

Los fabricantes de dispositivos de seguridad diariamente están actualizando sus dispositivos con nuevas firmas IPS para que, a través del análisis del tráfico que viene de la red WAN, pueda proteger la red frente a intrusiones y ataques.

Estas son algunos de las tareas a tener en cuenta en la puesta en marcha del filtro IPS:

- ✓ Habilitar el escaneo IPS para todos los servicios
- ✓ Mantener habilitadas las actualizaciones de firmas IPS
- ✓ No usar perfiles predeterminados; se debe crear perfiles de seguridad con firmas que necesite, según los servicios que va proteger
- ✓ Se debe tener activada la opción de auditoría, para llevar el registro de anomalías

- ***Bloquear descarga de archivos de extensión .exe, .jar, .bin, .msi en correo electrónico***

Bloquear la descarga de archivos por correo electrónico que contenga las siguientes extensiones: .exe, .jar, .bin, .msi, pues son archivos ejecutables que pueden desencadenar la ejecución del malware.

DETECTAR

- ***Chequeo continuo de los logs***

Los dispositivos de seguridad perimetral almacenan registros de eventos que permiten determinar en un momento de falla o ataque una información amplia de la situación que facilite la revisión de lo presentado en tiempo real. El análisis constante de los logs de un firewall es fundamental en la evaluación de riesgos de seguridad; además, permite iniciar de manera oportuna acciones de protección.

RESPONDER

- ***Definir procedimiento de actuar ante un incidente.***

En caso de un evento, deben estar definidos qué personas de la organización deben reaccionar en un evento. Los incidentes posibles comprenden diferentes categorías, tales como: compromiso de la integridad del sistema, negación de los recursos del sistema, acceso ilegal a un sistema por penetración o intrusión, uso malicioso de los recursos del sistema o cualquier otro tipo de daño a un sistema.

El manejo de un incidente se seguridad involucra 6 fases: protección del sistema, identificación del problema, contención del problema, erradicación del problema, recuperarse del incidente y el análisis de seguimiento.

Cuando ocurre un incidente varias personas estarán involucradas incluso es importante contar con un proveedor externo para obtener un segundo nivel. La seguridad personal en informática será la responsable de coordinar las actividades a ejecutar en el momento en que ocurra un incidente y, además, de asignar personas que ejecuten labores determinadas del proceso de manejo de incidentes. Cuando el incidente sea menor, sólo el personal interno se verá involucrado; por otra parte, en incidentes graves se podrá involucrar de manera adicional al proveedor externo que se tenga contratado. Se debe dejar registro de cada evento y actividades ejecutadas en la revisión y solución del incidente.

Una vez sea solucionado el incidente, es importante realizar un análisis; una fase de seguimiento, debido a que

esta comprende la evaluación y discusión de lo ocurrido, y así se pueden tomar las medidas necesarias para mitigarlo.

Se definen como procedimientos que permiten tener claridad sobre cómo actuar cuando ocurre un incidente de infección:

1. Aislar el equipo o sistema infectado
2. Registrar todas las acciones
3. Notificar al personal responsable
4. Identificar el problema
5. Determinar y eliminar cualquier proceso sospechoso
6. Inocular el sistema
7. Retornar al modo de operación normal
8. Análisis de seguimiento

RECUPERAR

- ***Copias de seguridad de configuración.***

  Se debe conservar un respaldo de la configuración de los dispositivos de seguridad, cada que se realice un cambio; esto, con el fin de tener un punto de restauración en el tiempo, en caso de una falla no esperada.

3.2 POLÍTICAS PARA PROTECCIÓN DE ENDPOINT FRENTE AL RANSOMWARE

A diferencia de la protección perimetral, la protección a nivel de Endpoint consiste en el aseguramiento de los host o dispositivos móviles; es decir, equipos tales como desktop, portátiles, servidores, entre otros. Estos dispositivos también cuentan con una serie de políticas que, si son aplicadas adecuadamente, pueden dar una capa adicional de seguridad y mitigar amenazas de tipo crypto Ransomware.

Empresas del mercado de seguridad, tales como McAfee, Trendmicro, karpesky, Fortinet, symantec, tienen expertos que, continuamente, están investigando y realizando aportes en sus blogs y revistas de seguridad acerca de la mitigación del riesgo. Mcafee labs, en su reporte de septiembre de 2016, indica la unión de diferentes empresas del sector "*nos unimos a Europol, La policía nacional holandesa y Kaspersky Lab para lanzar La iniciativa No More Ransom, un esfuerzo cooperativo Entre el orden público y el sector privado para luchar contra Ransomware*"**.** (Mcafee Labs, 2016)

Las políticas descritas a continuación fueron realizadas basadas en publicaciones de la CSRIT (WWW.CSIRT.ORG), en su apartado CSIRT Sample Policies ,se usaron documentos tales como (Guidelines on Anti-Virus Process , Audit Policy, Information Sensitivity Policy, Password Policy), también se usó documentos de buenas prácticas de hardening en dispositivos Fortigate (Handbook-HardeningyourFortiGate).

POLÍTICAS ENDPOINT
IDENTIFICAR
• ***Reducir cantidad de cuentas administrativas en la red.*** Mediante el uso o implementación de un menor número de cuentas administrativas, las cuales deben de contar con contraseñas de alto nivel para acceso a la red o información de la compañía, se introduce una capa adicional de protección para evitar que el malware pueda ser ejecutado con altos privilegios en uno de los equipos que comparten la conexión; previniendo su propagación en los dispositivos que se encuentren dentro del mismo segmento con posible vulnerabilidad. • ***Permita que se visualicen las extensiones ocultas de los archivos.*** Con frecuencia, una de las maneras en que se presenta Cryptolocker es en un archivo con extensión ".PDF.EXE", aprovechando la configuración predeterminada de **Windows** de ocultar las extensiones para tipos de archivos conocidos. Si desactiva la casilla correspondiente, podrá ver la extensión completa de cada uno y será más fácil detectar los archivos sospechosos.
PROTEGER
• ***Actualizar el sistema operativo de los equipos.*** Constantemente se lanzan actualizaciones y parches de seguridad, con el fin de eliminar las brechas en el sistema operativo de los equipos, debido a que un software desactualizado, es sinónimo de un software vulnerable, permitiendo ingresar de manera desapercibida y silenciosa.

Es recomendable tener habilitadas las actualizaciones automáticas del sistema. Los parches de seguridad tienen la particularidad de la perspectiva de que se deben aplicar de manera inmediata, pero éstos hacen parte de las actualizaciones relativas. No obstante, cuando el inconveniente sea notable y afecte directamente la seguridad del equipo, se debe aplicar el parche con urgencia; para reforzar esta buena práctica es necesario que un administrador de red realice un análisis general de los equipos validando las últimas actualizaciones de los sistemas operativos de las máquinas. En caso de que se presente alguna sin actualizar, este usuario, con permisos o privilegios elevados debe ejecutar su actualización de forma manual. De esta forma se podrá garantizar un control de actualizaciones y parches que previenen las vulnerabilidades de la red.

- ***Restringir los derechos administrativos locales***

Mediante un control de dominio o restricción de permisos en los usuarios locales, entre los cuales debe estar la conexión de dispositivos externos e instalación de software no autorizado por la empresa, se puede generar una protección adicional a nivel local. De esta manera se puede evitar que la amenaza de Ransomware se ejecute como administrador local y pueda propagarse sin ninguna restricción; garantizando de esta forma que no podrá modificar archivos ni recursos compartidos o en el sistema local.

- ***Restringir la iniciación de archivos ejecutables desde la carpeta descargas***

Una vez el usuario ha realizado la descarga, sea de un archivo adjunto de correo electrónico o una descarga en una página web, en la mayoría de casos el archivo irá a la carpeta descargas; el usuario ejecutará este archivo sin conocer si es un archivo malicioso. De tal manera puede iniciar el proceso de infección. Aplicando esta política, se reduce el tipo y el nivel de riesgo que pueda generar un usuario desprevenido.

- ***Educar a los empleados***

Los empleados de las compañías juegan un papel fundamental para la defensa ante ataques Ransomware, debido a que la mayoría de infecciones es generada por abrir un archivo adjunto contaminado, compartido a través de correo electrónico, visita de enlaces compartidos, descargas y navegación web.

Por lo tanto, se debe educar o capacitar de forma periódica a los empleados para que sean conscientes de las posibles consecuencias de hacer clic en ciertos enlaces, y reconocer el peligro inminente que estos pueden generar, para evitar ser infectados.

El personal de TI debe estar actualizado con las últimas noticias informáticas; en base a éstas se deben programar capacitaciones junto a los supervisores o jefes inmediatos del personal con acceso a la red e información sensible de la compañía. Con esta buena práctica se puede reducir en gran parte la amenaza de infección o ataque pues los usuarios son el primer filtro; y para los medios directos, de ataque como son dispositivos externos infectados o archivos en correos maliciosos, entre otros.

- ***Otorgar permisos de sólo lectura a ciertas carpetas compartidas***

Cuando se comparten recursos en la red, se debe conceder acceso sólo a las cuentas de usuario que necesiten modificar esos archivos; a las demás cuentas únicamente se les debe dar acceso de sólo lectura, en caso de que se requiera consultar la información. De esta manera se reduce la superficie de ataque del crypto Ransomware.

- ***Tener un antivirus actualizado***

Los equipos cliente deben tener la protección de su antivirus activada con análisis en tiempo real. Es una buena práctica que mensualmente se realice un escaneo bajo demanda de todo el sistema, para identificar amenazas en sectores poco comunes del sistema; sin embargo, se puede programar el antivirus para que ejecute un análisis automático superficial semanal, como control a posibles amenazas pequeñas que se puedan presentar; no obstante, esto implica que las firmas del antivirus

deben se actualizadas a diario.

- ***Firewall de host***

Al igual que los dispositivos perimetrales, los equipos y servidores tienen la opción de usar sus propios sistemas de firewall; deben estar habilitados y utilizarlos como filtro a puertos que sólo serán usados por aplicaciones legítimas de la organización; adicionalmente, los diferentes firewalls que se encuentren en la red deben trabajar en conjunto pues, de lo contrario, podrían entrar en conflicto sus políticas, conllevando a un bloqueo total o permitir todo de forma innecesaria.

- ***Protección web***

Los equipos de una organización se componen también de computadores portátiles que no siempre estarán dentro de la organización; por tanto, no serán protegidos por los sistemas de seguridad perimetral; es por esto que deben tener activos sus sistemas de filtrado web a nivel de host, para evitar que usuarios accedan a páginas peligrosas o que no tengan que ver con el trabajo de la organización. De esta forma se evitará un posible riesgo de infección de malware, que posteriormente, al ingresar a la red interna de la compañía, sería un foco de ataque o infección para los demás equipos de la red y con esto, la pérdida de la información; por lo tanto, estos equipos deben ser revisados con periodicidad por el personal de TI, para garantizar la integridad de los que pueden estar fuera de la organización.

DETECTAR

- ***Chequeo continuo de los logs.***

La consola de administración de seguridad de los dispositivos Endpoint almacena registros de eventos que permiten determinar una falla o ataque de manera amplia; una situación para facilitar la revisión de lo presentado en tiempo real. El análisis constante de los logs es fundamental en la evaluación de

riesgos de seguridad, debido a que permite almacenar, catalogar, constituir y analizar, permitiendo iniciar de manera oportuna acciones de protección. Con esto se espera el descubrimiento de vulnerabilidades, inconvenientes en el software, ataques o brechas de seguridad, generando métodos para acciones que faciliten estar al tanto, de manera oportuna, de la gravedad del caso y/o de la existencia de equipos afectados.

El análisis de la información obtenida de los logs facilita la administración y servicio, ya que, en el momento que se presente un evento de comportamiento anormal, se está enterado de lo que va sucediendo, desde su inicio hasta la solución final de la novedad.

RESPONDER

- ***Definir procedimiento de actuar ante un incidente.***

En caso que se presente alguna eventualidad, se deben tener claros los roles y las personas de la organización, que deben reaccionar en al evento. Adicionalmente, se debe contar con un proveedor externo, cuya función será la de ser el segundo nivel, brindando apoyo para resolver la novedad.

RECUPERAR

- ***Realizar copias de seguridad periódicas de la información***

Realizar respaldo de la información y los sistemas, de manera continua, resultan fundamentales en el momento de pérdida de datos; además, es de suma importancia el almacenamiento de las copias de seguridad.

Se debe verificar que los procedimientos de copias de seguridad se estén realizando de manera correcta, y que la restauración sea aplicable y funcional en la infraestructura de la compañía. Se debe tener en cuenta que algunas de las soluciones actuales de copias de seguridad en nube, de igual manera son vulnerables a ataques Ransomware. En algunas ocasiones las copias de seguridad sobrescriben la información que ya ha sido infectada por Ransomware, generando el cifrado de los

datos; por tal motivo, es importante que dichas copias no sean solo locales; se debe garantizar diferentes medios de copia y lugares de almacenamiento, en especial cuando la información es sensible para la organización.

3.3 PROCEDIMIENTO DE RECUPERACIÓN POST-INCIDENTE

Diagrama Post incidente

En caso de un incidente donde las capas de protección no pudieron contener la infección y la integridad de los datos se vieron comprometidos, se debe activar el plan de recuperación, con el fin de tener los datos nuevamente disponibles y en su estado inicial. En la figura 23 se realiza una descripción del esquema de recuperación post-incidente.

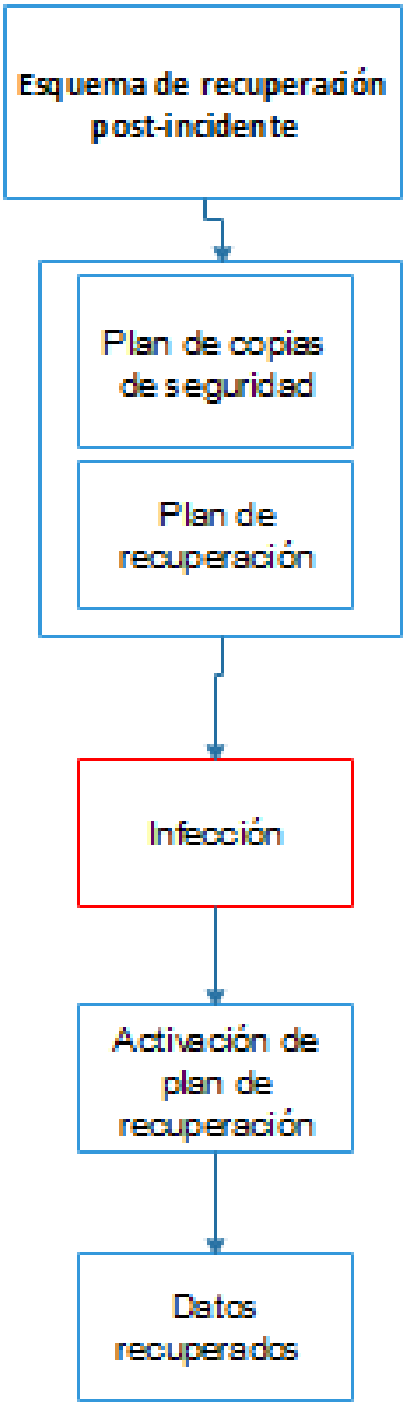

Figura 23. Diagrama Post incidente. Fuente Autores

Plan de recuperación

A continuación, se describe una serie de procedimientos que fueron realizados, basados en la NIST Special Publication 800-34, con el fin de trazar un plan de recuperación de un servidor de archivos, en caso de que las capas de protección expuestas anteriormente no puedan contener la infección de Crypto Ransomware y los datos contenidos en el servidor de archivos se vean comprometidos.

1. Introducción

Los datos de las organizaciones son vitales; por lo tanto, es fundamental que los servicios proporcionados por el servidor de archivos sean capaces de operar eficazmente y sin interrupciones excesivas. Este plan establece procedimientos para la recuperación de un servidor de archivos, de forma rápida y eficaz.

1.1 Ámbito

Este plan establece procedimientos para recuperar un servidor de archivos, después de una interrupción. Se han establecido los siguientes objetivos del plan de recuperación:

- ✓ Maximizar la efectividad de las operaciones de contingencia, a través de un plan establecido que consta de las siguientes fases:

  - ***Fase de activación y notificación***: para activar el plan y determinar el grado de daño

  - ***Fase de Recuperación***: Para restaurar los datos del servidor de archivos

- ***Fase de reconstitución***: para asegurarse, mediante pruebas, que el servidor de archivos se encuentra en su estado normal, y que se reanudan las operaciones normales.

✓ Identificar actividades, recursos, procedimientos y requisitos de procesamiento, durante interrupciones prolongadas.

✓ Asignar responsabilidades al personal designado de la organización y proporcionar instrucciones para recuperar el servidor de archivos, durante períodos prolongados de interrupción de las operaciones normales.

2. Operaciones

Esta sección proporciona detalles sobre el servidor de archivos; una descripción general de las tres fases de activación, notificación, recuperación y una descripción de las funciones y responsabilidades del personal de la Organización durante una activación del plan.

2.1. Descripción del sistema

El esquema de almacenamiento se compone de los siguientes elementos listados a continuación:

Servidor de Archivos

Es un equipo configurado, con el fin de almacenar y gestionar la administración de datos en una organización; el modelo que utiliza para este servicio se basa en cliente/servidor. Cuando los usuarios de la red necesiten un archivo, podrán acceder a éste a través del servidor de archivos, sin necesidad de pasarlo manualmente por medios extraíbles. Existen diferentes protocolos utilizados por servidores de estos para la transferencia de archivos entre clientes y servidores.

NAS (Dispositivos de Almacenamiento en Red)

Es un dispositivo de almacenamiento, conectado a una red que permite almacenar y ubicar los datos en un punto centralizado, para usuarios autorizados de la red. Los dispositivos NAS son flexibles y expandibles; esto significa que, a medida que vaya necesitando más capacidad de almacenamiento, podrá añadirla a lo que ya tiene.

Un dispositivo NAS es como tener una nube privada en la oficina. Es más veloz, menos costoso y brinda todos los beneficios de una nube pública. En la figura 24 se observa el esquema de almacenamiento de la copia de seguridad.

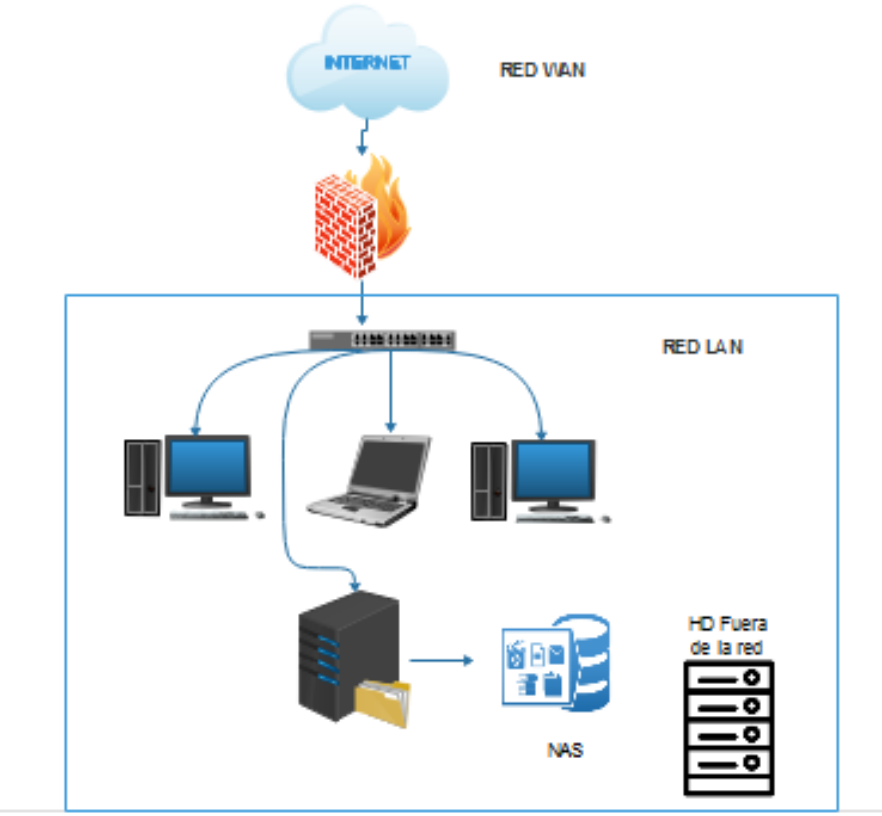

Figura 24. Esquema de almacenamiento. Fuente Autores.

El servidor de archivos de la organización tiene un sistema operativo windows server 2012 y será quien tenga todos los directorios de la información que usan los usuarios de la red. Los permisos asociados a quien puede acceder a estos archivos serán otorgados por el área de sistemas de la empresa. La Nas compartirá una red con el servidor de archivos, con el fin de almacenar las copias de seguridad del SA.

2.2 Descripción de 3 Fases

Este plan se ha desarrollado para recuperar y reconstruir un servidor de archivos, utilizando un enfoque de tres fases. Este enfoque asegura que los esfuerzos de recuperación y reconstrucción del sistema se realicen en una secuencia metódica para maximizar la efectividad de los esfuerzos de recuperación y reconstitución, y minimizar el tiempo de interrupción del sistema debido a errores u omisiones.

Las tres fases de recuperación del sistema son:

Fase de Activación y Notificación: La activación del plan de recuperación ocurre después de una interrupción o evidencias de una encriptación de archivos por parte de un malware. El evento de interrupción puede ocasionar daños graves a las instalaciones que albergan el sistema, o a los archivos que allí se alojan.

Una vez que se activa el PR (plan de recuperación), se notifica a los propietarios y usuarios del sistema de una posible interrupción a largo plazo y se realiza una evaluación completa de la interrupción del sistema. La información de la evaluación de interrupción se presenta a los propietarios del sistema

Fase de recuperación: la fase de recuperación detalla las actividades y los procedimientos para la recuperación del sistema afectado. Las actividades y los procedimientos se escriben a un nivel tal, que un técnico debidamente capacitado pueda recuperar el sistema sin conocimiento previo de este.

***Reconstrucción*:** define las acciones tomadas para probar y validar la capacidad y la funcionalidad del sistema en la ubicación permanente original o nueva. Esta fase consiste en dos actividades principales: validar la reconstrucción exitosa y la desactivación del plan.

Durante la validación, el sistema se prueba y valida como operativo antes de devolver la operación a su estado normal. El sistema se declara recuperado y operativo por los propietarios del sistema, al completar con éxito las pruebas de validación.

La desactivación incluye actividades para notificar a los usuarios del estado operacional del sistema.

2.3 Roles Responsabilidades

El plan establece varias funciones para la recuperación del servidor de archivos. Las personas o los equipos asignados a las funciones deben ser capacitadas para responder a un evento de contingencia que afecte el sistema.

- ✓ **Responsable manteniendo del plan de recuperación**: esta persona deberá estar encargada de actualizar todos los procedimientos del plan de recuperación basado en experiencias anteriores o nuevos procesos que puedan ayudar a la mejora de tales procedimientos.
- ✓ **Responsable de copias de seguridad:** Esta persona debe estar encargada de la ejecución y la supervisión del plan de copias de seguridad; debe realizar la programación en el servidor de archivos y proporcionar todas las configuraciones necesarias para esto. También debe estar al tanto de que se estén llevando a cabo las copias de seguridad en los tiempos estipulados, y realizar las tareas de restauración asignadas.
- ✓ **Coordinador de Recuperación**: Esta persona será la encargada de dar inicio al plan de recuperación; según los procedimientos diseñados para esto, será el encargado de comunicar a las demás áreas el inicio de procedimientos de recuperación y trabajará de la mano con las demás áreas para que se aplique el PR**.**

3. Activación y Notificación

La fase de activación y notificación define las acciones iniciales tomadas una vez que se ha detectado una interrupción o se ha perdido la integridad de los datos en el servidor de archivos. Esta fase incluye actividades para notificar al personal de recuperación, realizar una evaluación de interrupciones y activar el plan. Al finalizar la Fase de Activación y Notificación, el personal del PR estará preparado para realizar medidas de recuperación.

3.1 Criterios de Activación

El PR puede activarse, si uno o más de los siguientes criterios son reunidos:

1. El tipo de interrupción indica que el servidor de archivos estará por fuera más de 1 hora.

2. Se verifica y se evidencia que uno de los ficheros ha perdido su integridad, y ha sido encriptado por una variante de Crypto Ransomware.

3. El arranque del sistema operativo ha sido encriptado, y no se puede iniciar.

3.2 Notificación

El primer paso, después de la activación del PR, es la notificación del personal de soporte apropiado. La información de contacto se debe incluir en la siguiente tabla:

Personal clave en el plan de recuperación		
Personal Clave	**Información De Contacto**	
Responsable De Copias De Seguridad	Trabajo	
	Casa	
	Celular	
	Email	
Coordinador De Recuperación	Trabajo	
	Casa	
	Celular	
	Email	
Responsable Manteniendo Del Plan De Recuperación	Trabajo	
	Casa	
	Celular	
	Email	

Tabla 4. Personal clave en el plan de recuperación. Fuente: Autores

3.3 Evaluación de la interrupción

Luego de la notificación, se necesita una evaluación completa de la interrupción, para determinar su alcance y el tiempo de recuperación esperado. Esta evaluación de interrupción se lleva a cabo por el área de seguridad informática. Los resultados de la evaluación se proporcionan al coordinador de Recuperación, para ayudar en la puesta en marcha del servidor de archivos.

1. En caso de que se haya afectado el inicio del sistema operativo, validar el mensaje que es mostrado.
2. Junto con el personal técnico de la empresa, sustentar que el daño sí es causado por una infección de malware
3. Una vez realizada la confirmación, se dará un tiempo estimado de máximo 2 horas para su restauración.
4. En caso de que se hayan visto comprometidos ficheros del servidor de archivos.
5. Verificar cuáles ficheros han sido alcanzados por el malware
6. Una vez identificados, realizar una lista para su posterior restauración
7. Se tendrá un tiempo estimado de 1 hora para realizar la restauración
8. Los elementos necesarios para la restauración será tener una conexión a la NAS de almacenamiento en red o las cintas de backup con los archivos más recientes de éstas.

4. Recuperación

Esta Fase proporciona operaciones de recuperación que comienzan después de que se ha activado el PR, se han completado las evaluaciones de interrupción, se ha notificado al personal y se han movilizado los equipos apropiados. Las actividades de la fase de recuperación se centran en la implementación de estrategias de recuperación para restaurar las capacidades del sistema, reparar daños y reanudar las capacidades operativas en la ubicación original o alternativa. Al finalizar la Fase de Recuperación, el servidor de archivos será funcional y capaz de realizar las funciones identificadas en la Sección 2.1 de este plan.

4.1 Secuencia de las actividades de recuperación

Las siguientes actividades ocurren durante la recuperación del servidor de archivos

1. Identificación de los recursos necesarios para realizar la recuperación del sistema

2. Verificación de la conexión de Nas de almacenamiento y Cintas Necesarias.
3. Ubicación de copia de seguridad y medios de instalación.
4. Recuperación de hardware o sistema operativo, si es necesario
5. Recuperación del sistema o los archivos que ha sido afectados

4.2 Procedimientos de recuperación

Se proporcionan los siguientes procedimientos para la recuperación del servidor de archivos de un sistema operativo Windows. Es también aplicable a sistemas Linux. Los procedimientos de recuperación deben ejecutarse en la secuencia presentada, para realizar una recuperación eficiente.

Recuperación de archivos

1. Se evidencia que los archivos originales han sido comprometidos.

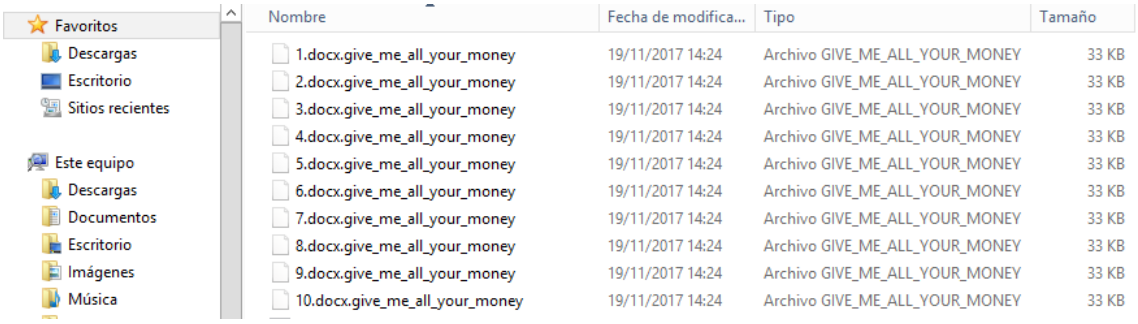

Figura 25. Archivos que perdieron su integridad. Fuente Autores.

2. Ubicar y tener a la mano los medios donde fue almacenada la copia de seguridad; para este caso, los archivos deben estar almacenados en la NAS de almacenamiento en red.

3. Ingresar a la consola de administración de acronis backup para dar inicio al proceso de recuperación de los archivos.

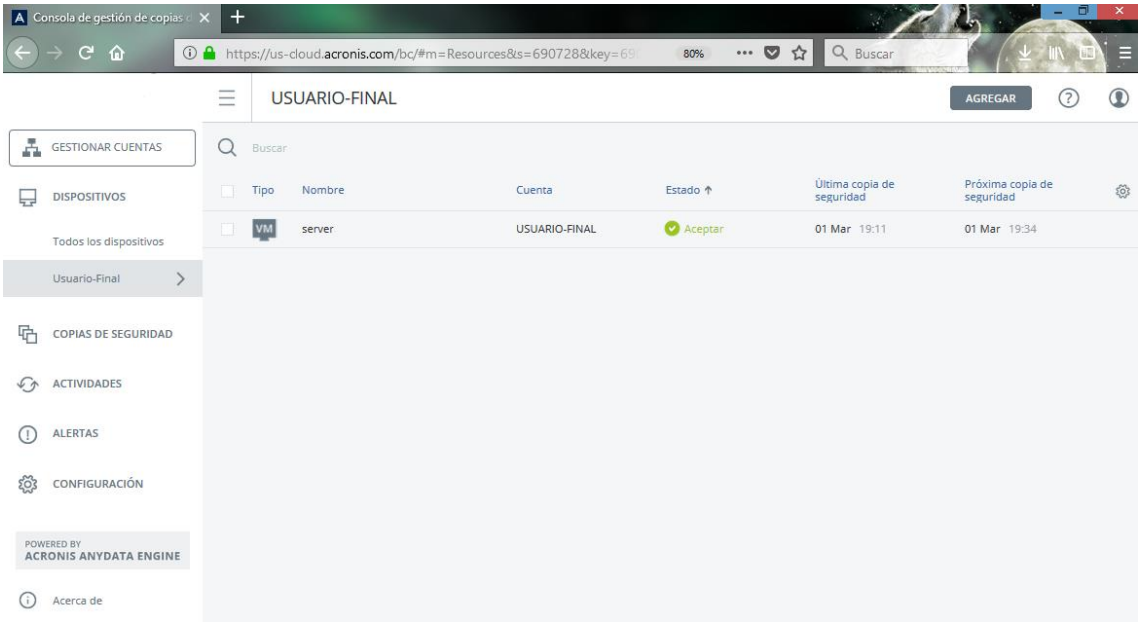

Figura 26. Consola de administración principal. Fuente Autores.

4. Se ingresa en la columna izquierda a la opción de copias de seguridad. Allí estará almacenado el historial de copias que se pueden recuperar.

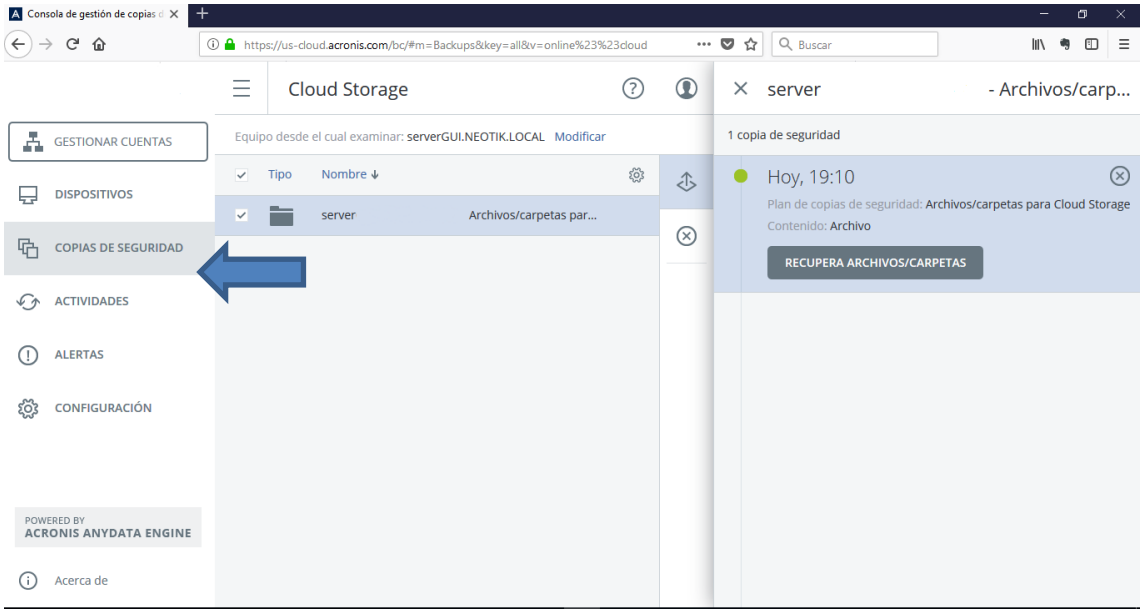

Figura 27. Procesos de recuperación de archivos. Fuente Autores.

5. Se selecciona la opción: recuperar archivos y carpetas.

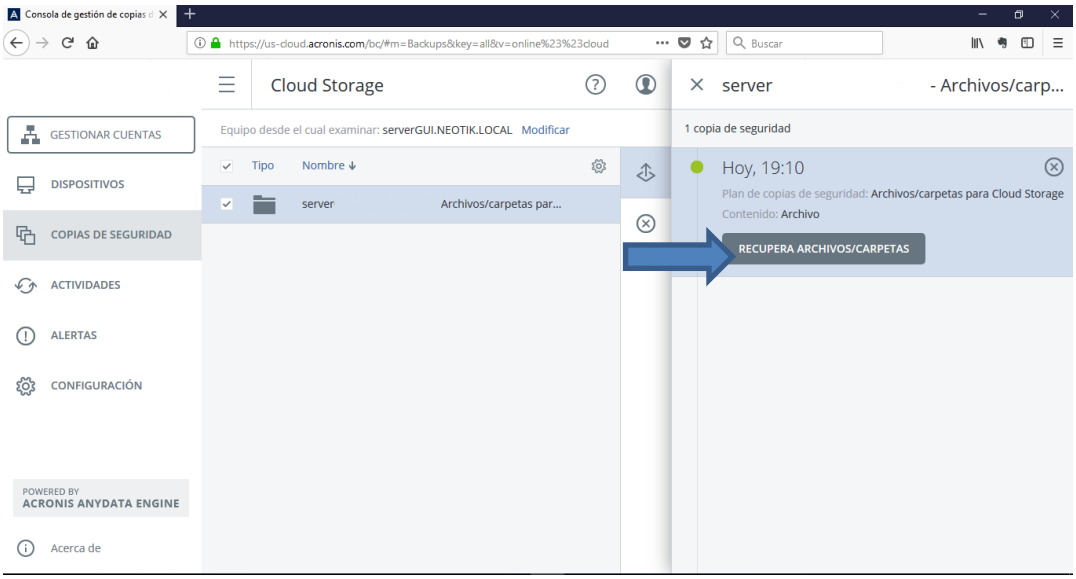

Figura 28. Procesos de recuperación de archivos. Fuente Autores.

6. En este paso, se debe seleccionar los archivos que se van a recuperar y luego dar clic en Recuperar.

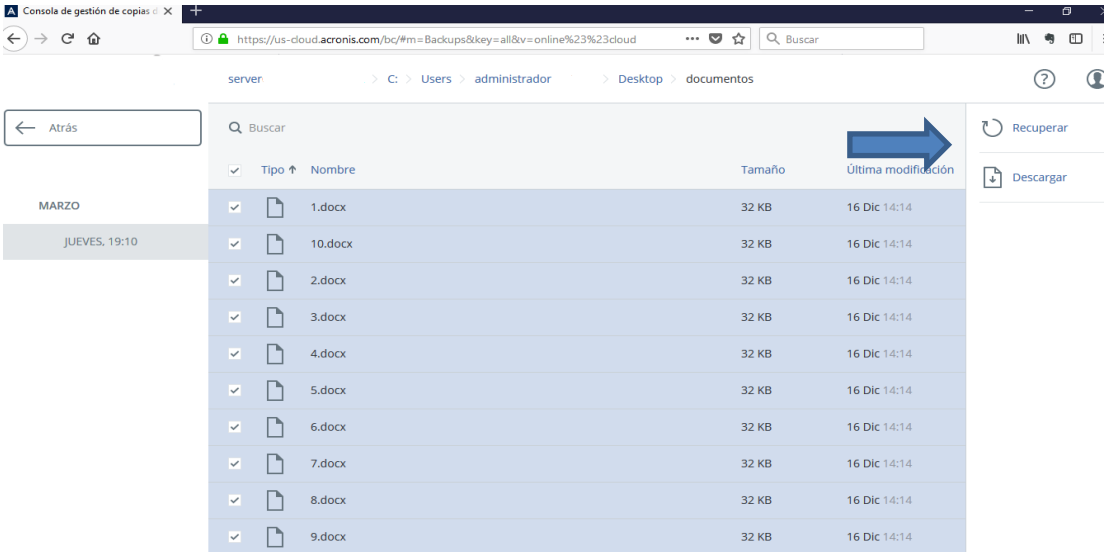

Figura 29. Procesos de recuperación de archivos. Fuente Autores.

7. Se puede seleccionar Recuperar en la ubicación original o en una ubicación alternativa; luego, dar clic en Recuperar.

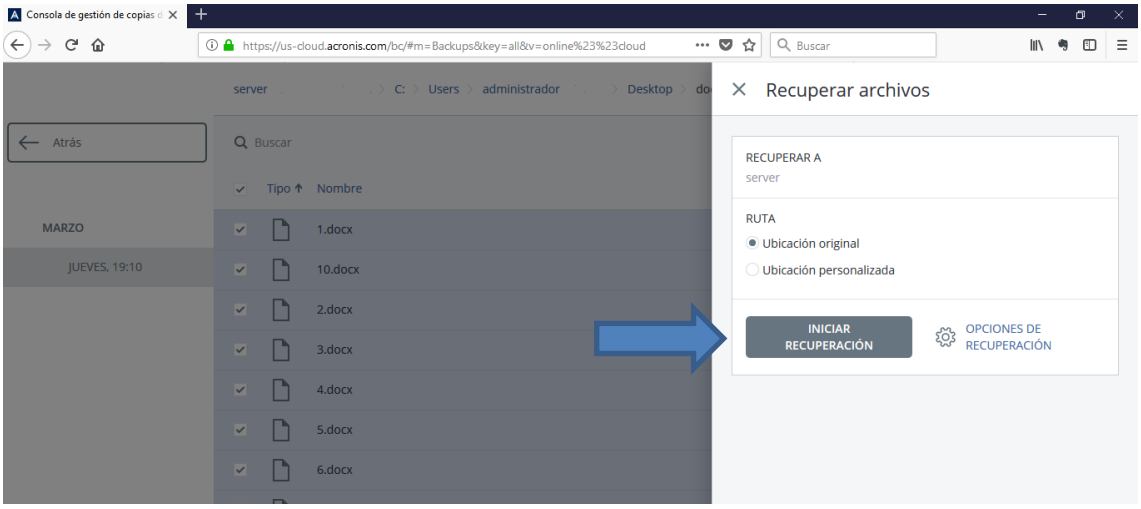

Figura 30. Procesos de recuperación de archivos. Fuente Autores.

8. Por último, se busca la ubicación original de los archivos y se comprueba que los datos estén en su estado correcto. En este paso se ha recuperado la integridad de los datos.

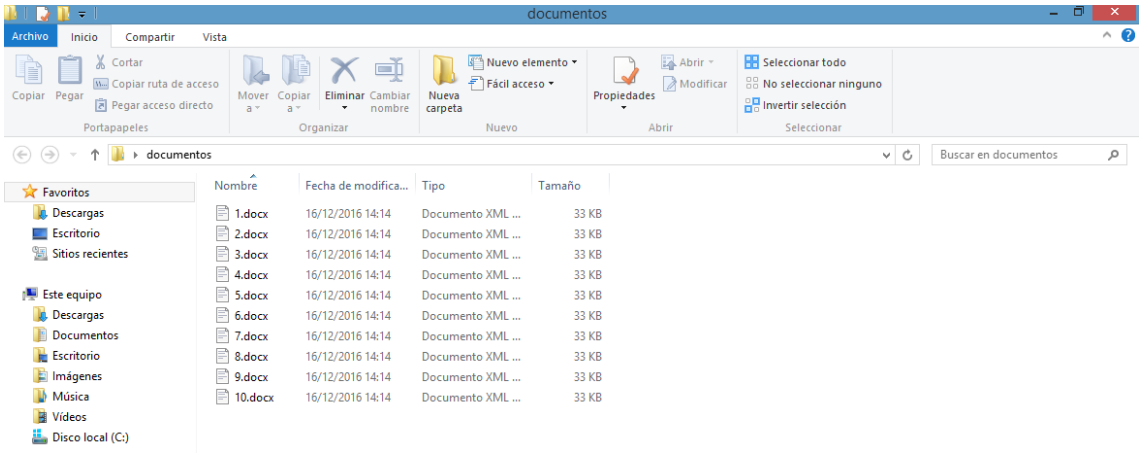

Figura 31. Archivos Recuperados a su estado original. Fuente Autores.

5. Restablecimiento

La fase de restablecimiento es el proceso por el cual se completan las actividades de recuperación y se reanudan las operaciones del sistema. La fase consiste en dos actividades principales: validar el restablecimiento y desactivación exitosa del plan.

5.1 Pruebas de validación

La prueba de datos de validación es el proceso de probar datos para asegurar que los archivos se hayan recuperado completamente en la ubicación permanente. Los siguientes procedimientos se utilizarán para determinar que los datos están completos y actualizados a la última copia de seguridad disponible.

1. verificar que el sistema operativo del servidor de archivos inicie correctamente; para esto se debe realizar un reinicio e iniciar sesión de nuevo, con las credenciales que se usaban antes del desastre.

2. Realizar un escaneo completo del servidor con el software antivirus que se utilice en el momento. Una vez finalizado el escaneo y este no haya arrojado datos de ninguna infección, se podrá validar que no existe una amenaza para iniciar la operación de nuevo.

3. Ingresar a una de las carpetas que anteriormente aparecían con doble extensión o que habían perdido su integridad. Si se verifica que no ha sufrido ningún cambio y se encuentra nuevamente en su estado normal .se podrá dar inicio a las operaciones en producción.

5.2 Declaración de recuperación

Al completar con éxito las pruebas y la validación, el Coordinador de recuperación declarará formalmente la recuperación, y el servidor de archivos entrará en operaciones normales.

5.3 Notificación a usuarios.

Una vez el servidor de archivos este en operación los usuarios serán notificados vía, correo electrónico llamadas telefónicas, etc.

5.4 Desactivación

Una vez todas las actividades han sido realizadas el coordinador de recuperación puede dar por finalizado el plan de recuperación. La notificación de esta declaración debe ser dada a todo el personal técnico y de negocio.

3.4 MAPEO DE POLITICAS Y PROCEDIMIENTOS CON EL ANEXO A17 DE LA NORMA ISO 27001:2013

En este apartado se realiza una relación entre las políticas y procedimientos propuestos anteriormente en este documento y la norma ISO 27001:2013 más específicamente el anexo A del control: continuidad de negocio.

En los apartados anteriores se desarrollaron políticas y procedimientos basados en las mejores prácticas y en marcos de referencia aceptados y propuestos por los mejores especialistas en el tema, el mapeo se realiza con el fin de llevar una correlación con la norma ISO 27001:2013 que es un estándar de seguridad de la información aceptado a nivel mundial. Los procedimientos tanto de recuperación, como de prevención deben compaginar para lograr el objetivo de preservar la seguridad de la información.

Las siguientes son algunas de las ventajas del seguimiento de la norma ISO 2007:2013 para asegurar la continuidad del negocio:

- Establecimiento de procedimientos.
- Revisión y pruebas de procedimientos.
- Concientización de la norma.
- Gestión de la continuidad del negocio.

4. RESULTADOS Y DISCUSIÓN

EJEMPLO PRÁCTICO DE CONFIGURACIÓN DE POLÍTICAS EN UN DISPOSITIVO UTM MARCA FORTIGATE 300D

Fortinet es una compañía a nivel mundial, dedicada a desarrollar y proveer software y equipos de seguridad de red. Su gama más conocida es Fortigate, un dispositivo UTM que posee funcionalidades tales como firewall, control de aplicaciones, VPN, filtrado web, entre otros, brindando seguridad a la red.

A continuación, se lista un ejemplo práctico donde se interviene un dispositivo UTM y se realizan las configuraciones en el dispositivo, que pretenden dar una primera capa de protección frente a amenazas de tipo Crypto Ransomware. Se da un título inicial que ilustra la política aplicada; se muestra con una imagen la configuración en el equipo y se menciona la ruta que se debe tomar para realizar la configuración.

Configuración de políticas en Fortigate:

- ✓ ***Actualización del software del dispositivo UTM, herramienta de antivirus y firmas IPS:*** a través de la licencia que se adquiere junto con el producto se reciben actualizaciones periódicas de las diferentes firmas de virus, las definiciones IPS Y firmware del UTM.

Ir a System > FortiGuard

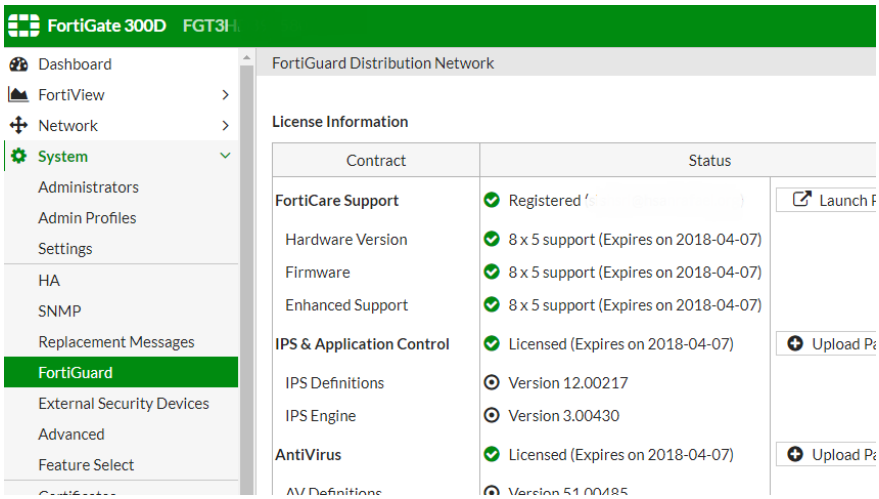

Figura 32.FortiGuard. Fuente Autores.

- ✓ ***Panel principal:*** la pestaña de security profiles contiene diferentes módulos que componen el UTM, incluyendo filtrado web, control de aplicaciones, antivirus, entre otros.

Figura 33. Perfiles de seguridad. Fuente Autores.

✓ ***Activado de filtrado web***

Los servicios de Fortinet cuentan con una base de datos de URL's de internet, las cuales clasifican los sitios según categorías; se deben activar aquellas categorías que ponen en riesgo la red interna, tales como riesgos de seguridad potencialmente peligrosas y contenido para adultos.

Ir a Security Profiles > Web Filter

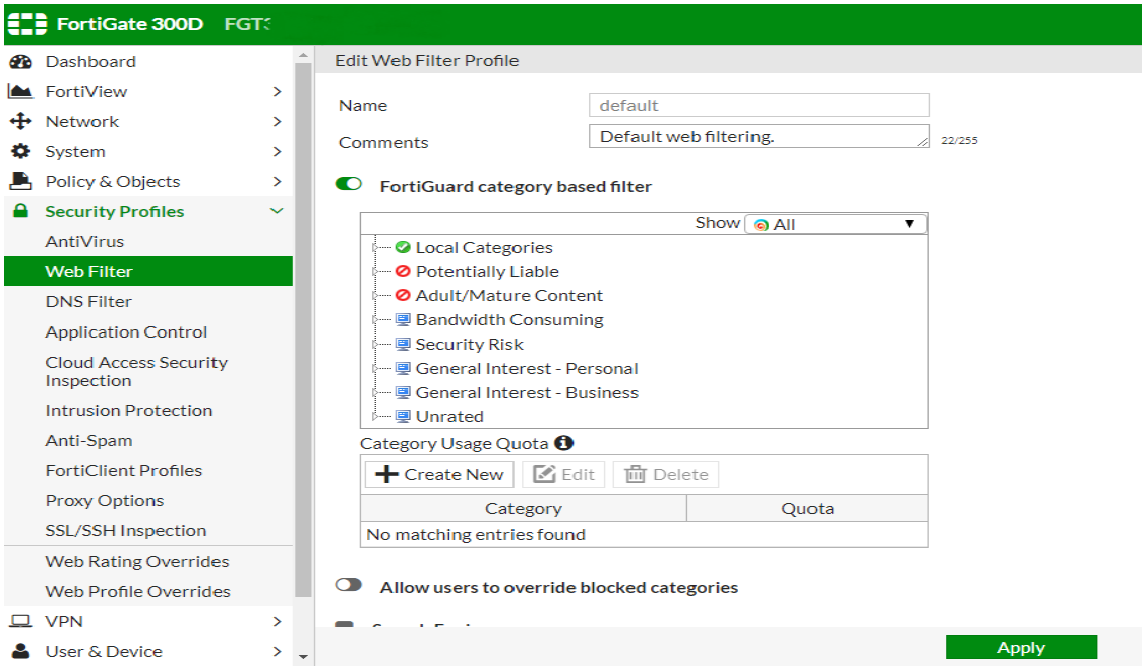

Figura 34. Filtro Web. Fuente Autores.

✓ ***Bloquear descarga de contenido malicioso:*** Activando el filtrado de esta categoría se evitará la descarga de software malicioso.

Ir a Security Profiles > Web Filter > Bandwidth Consuming > Freeware and software downloads

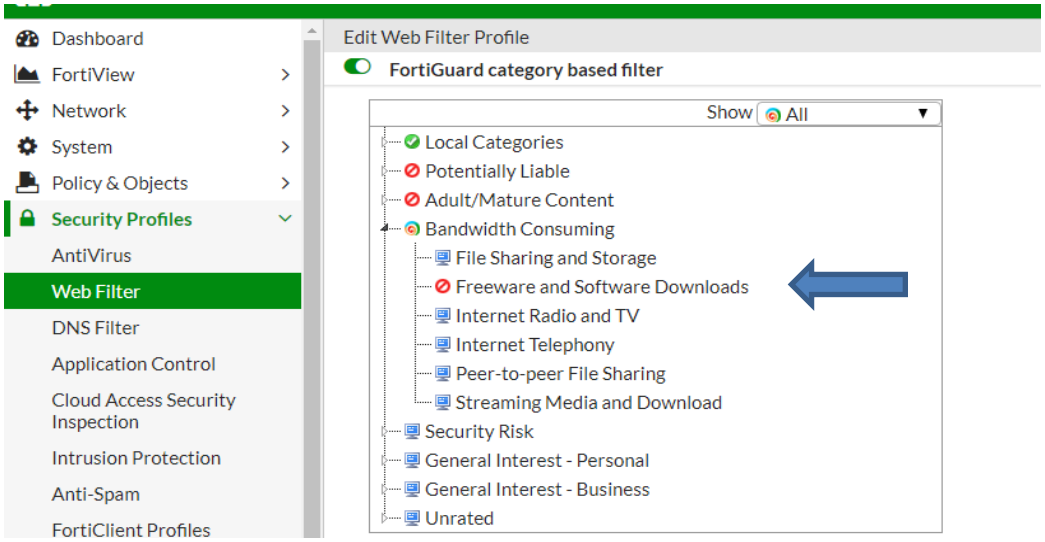

Figura 35. Filtrado de descargas. Fuente Autores.

- ✓ ***Activado de firewall de la red***

En esta pestaña se configuran las reglas de entrada y salida de tráfico, permitiendo sólo el tráfico a las direcciones conocidas que sean de procedencia segura.

Ir a Policy & Objects > IPv4 DoS Policy

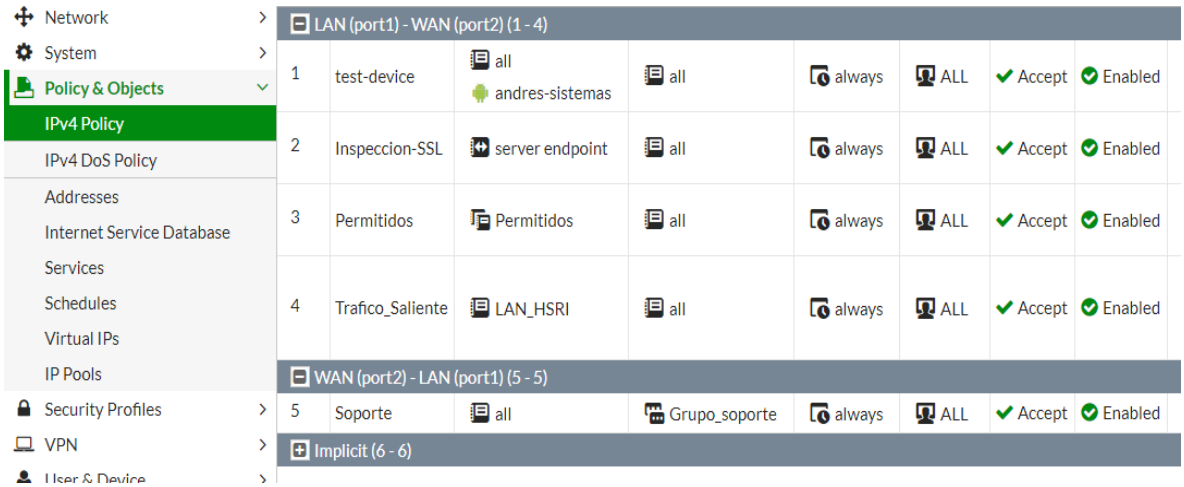

Figura 36. Reglas de excepciones. Fuente Autores.

- ✓ ***Usar filtros Antispam***

En esta pestaña se debe habilitar el filtro antispam, con el fin de limpiar la recepción del correo electrónico, de correos maliciosos y spam.

Ir a Security Profiles > Antispam

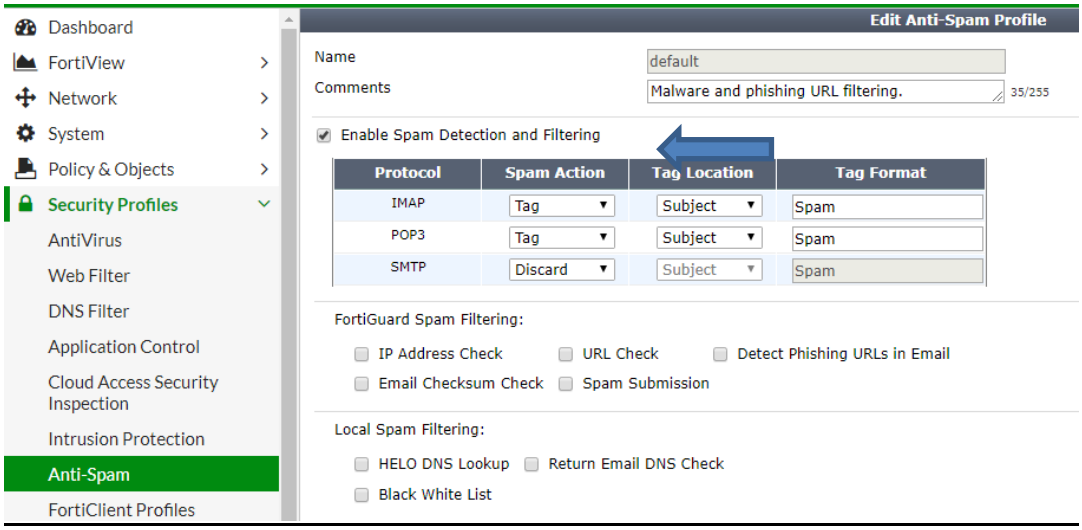

Figura 37. Filtros antispam. Fuente Autores.

- ✓ ***Usar filtros IPS***

En esta pestaña encontramos las firmas IPS que vienen por defecto del laboratorio de seguridad del fabricante Fortigate. Habilitando esta opción se previenen intentos de ingreso desde fuentes externas a la red.

Ir a Security Profiles > Intrusion Protection

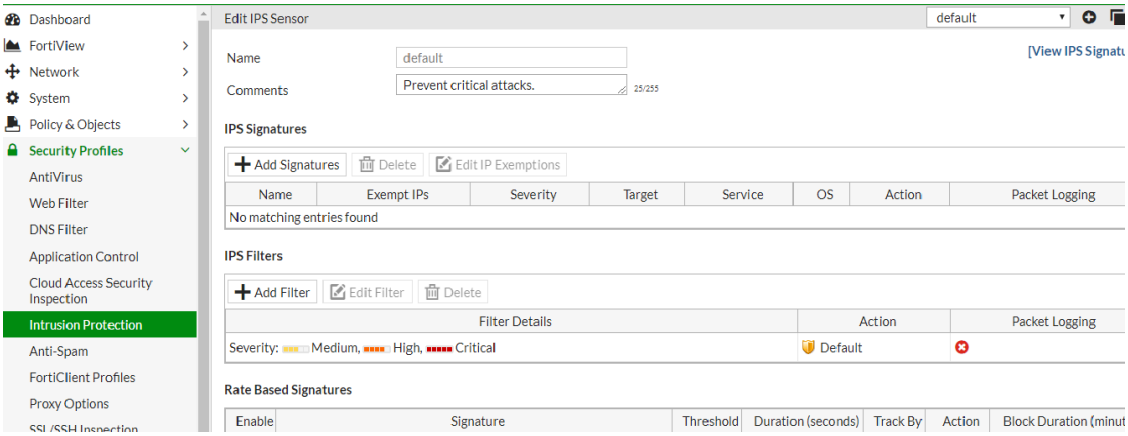

Figura 38. Reglas IPS. Fuente Autores.

- ✓ ***Política de Navegación***

A la poltiica general de navegacion deben ser agregados cada unos de los modulos que se han activado previamente. Esta politica será aplicada a todo el trafico saliente de la red ,permitiendo que cada uno de los filtros trabajen en conjunto.

Ir a Policy & objects > IPv4Policy

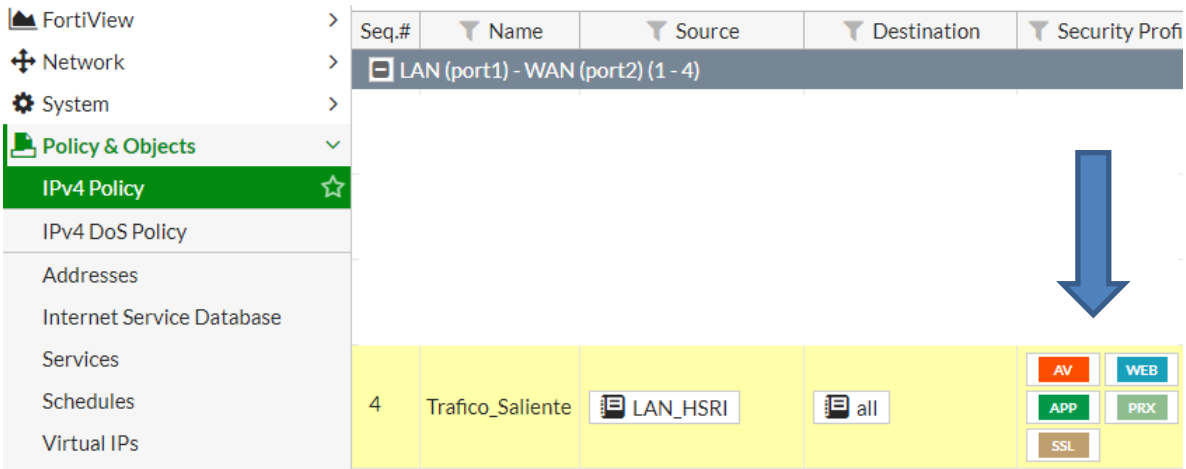

Figura 39. Políticas de navegación. Fuente Autores.

EJEMPLO DE CONFIGURACIÓN DE POLÍTICAS EN DISPOSITIVO DE ADMINISTRACIÓN DE SEGURIDAD ENDPOINT (CONSOLA MCAFEE)

McAfee Es una compañía en seguridad informática. Según el cuadrante GARTNER del año 2017, McAfee es la empresa líder en soluciones Endpoint. Su enfoque es la creación de productos para empresas y usuarios finales. Uno de los productos más destacados es la consola McAfee ePolicy Orchestrator (ePO), que es una solución de administración, desde donde se puede gestionar el software antivirus en las organizaciones.

- ✓ **Consola de administración EPO MCAFEE**

Es una consola de administración centralizada, desde la cual se pueden gestionar todos los equipos de la red en los cuales se tengan instalados agentes; estos agentes se comunican continuamente para llevar información referente a la seguridad de los dispositivos que está protegiendo.

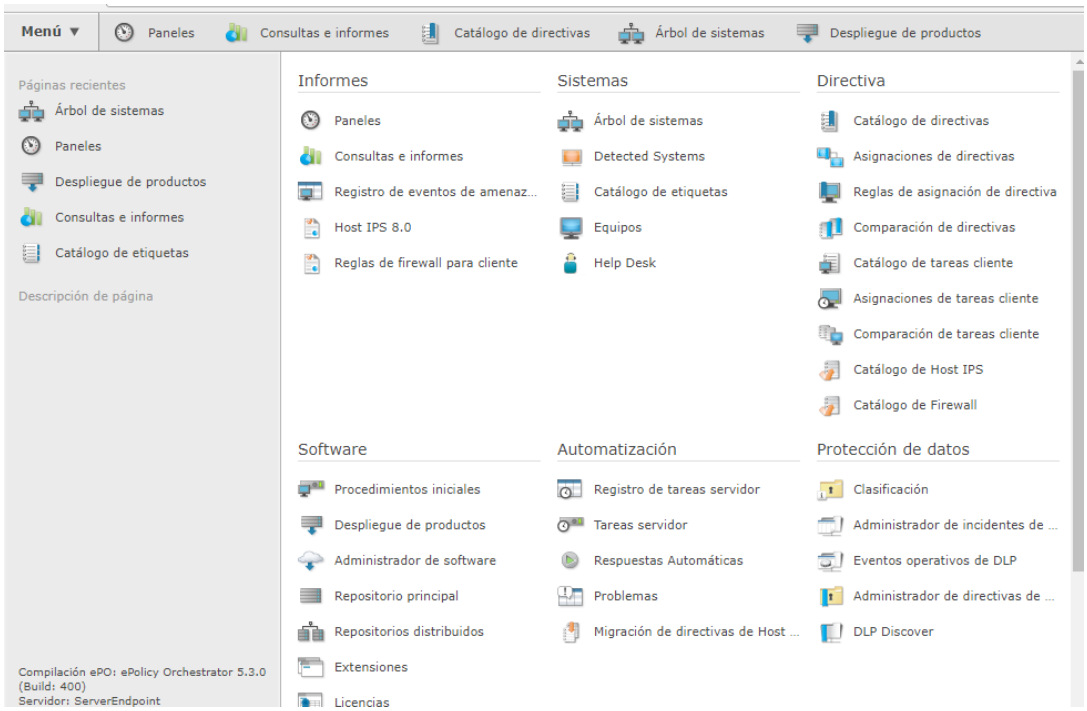

Figura 40. Políticas de navegación. Fuente Autores.

- ✓ ***Restringir la iniciación de archivos ejecutables desde la carpeta descargas***

  El Virusscan Enterprise es el antivirus de McAfee el cual se encarga de la protección de archivos maliciosos y virus. Uno de los campos de configuración del Virusscan son las directivas donde se establecen las funciones que éste tendrá sobre los equipos.

  Se debe activar las reglas de protección de acceso para prevenir la ejecución de archivos ejecutables, al ser realizadas en la carpeta descargas de los sistemas operativos windows.

Menú > Catalogo de directivas > prevención cryptolocker con bloqueo.

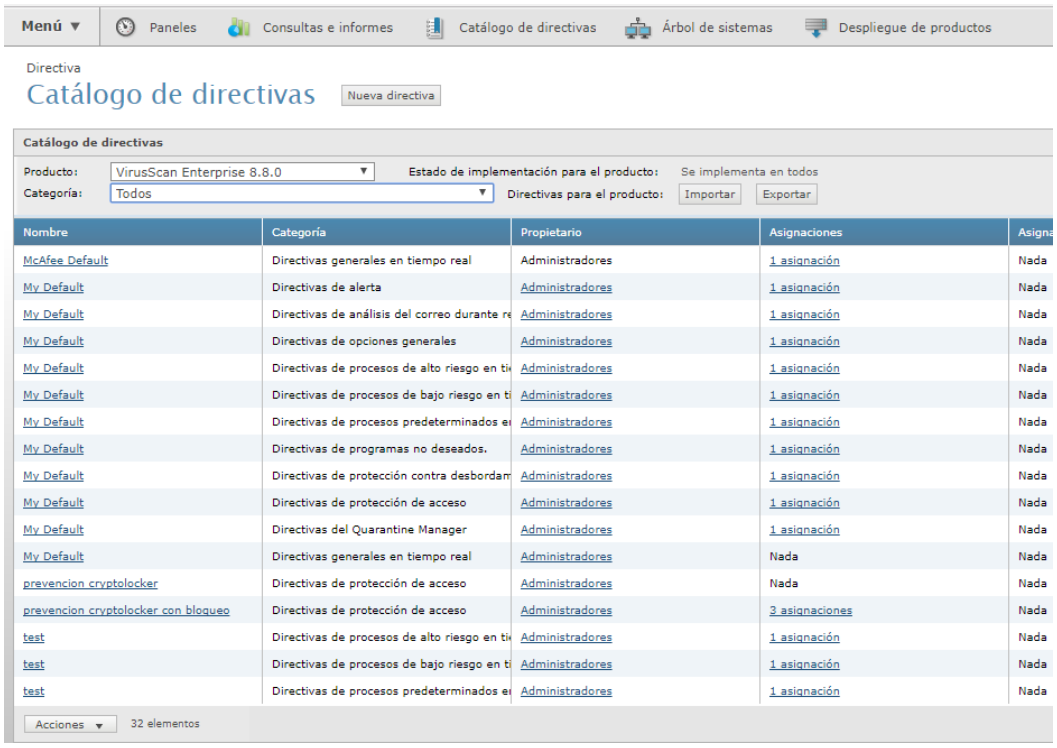

Figura 41. Catalogo de directivas. Fuente Autores.

Directivas de protección de acceso > prevención cryptolocker con bloqueo

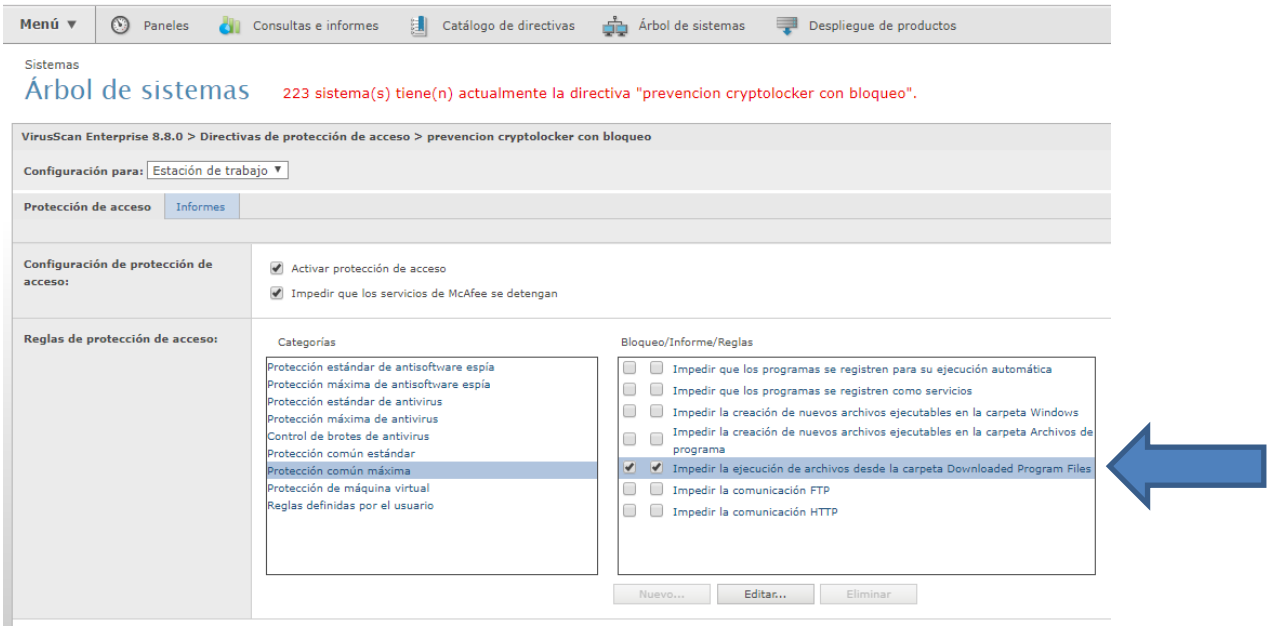

Figura 42. Políticas de navegación. Fuente Autores.

- ✓ ***Actualización de Firmas de Virus***

  Para que los antivirus puedan dar protección de manera adecuada, siempre deben tener sus bases de datos de virus a la última versión, también llamadas firmas de virus. Estos son archivos que diariamente actualiza McAfee y contiene toda la información relacionada con las amenazas en la red.

  Una vez se instala la consola, ésta, de manera predeterminada, actualiza diariamente todos los antivirus; se debe verificar que este archivo corresponda a la última versión.

Menú > Paneles > Resumen de ePO

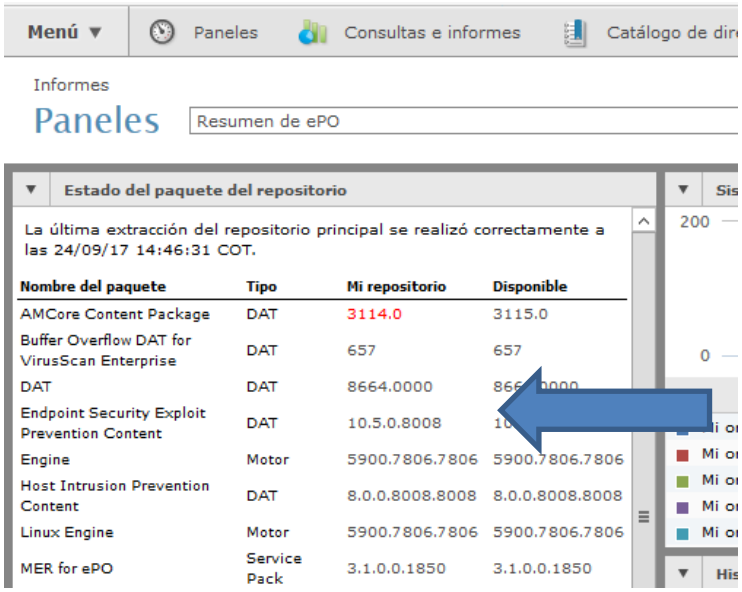

Figura 43. Políticas de navegación. Fuente Autores.

- ✓ ***Filtros de protección Activados***

  En el panel de usuario se debe asegurar que se encuentren activos todos los filtros de seguridad para una correcta protección de los dispositivos.

Panel de usuario > Administrar funciones > Virusscan

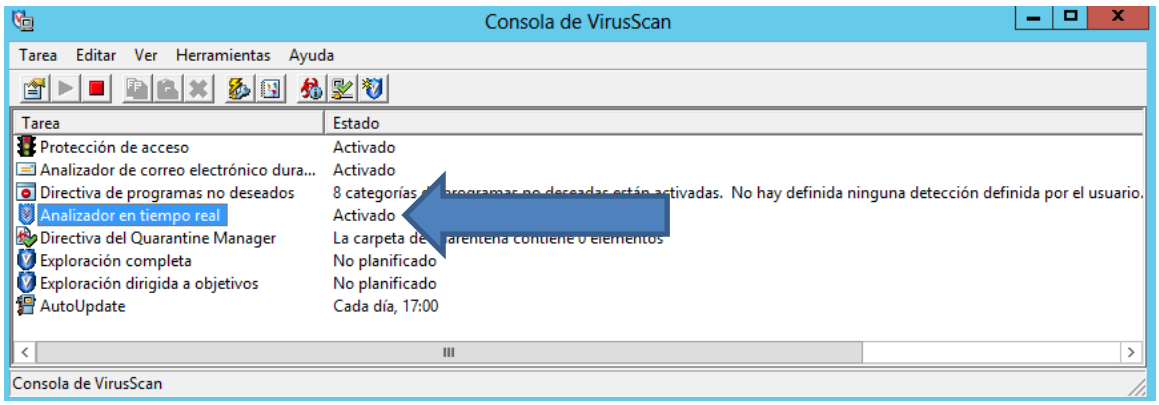

Figura 44. Consola de VirusSacan. Fuente Autores.

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

CONCLUSIONES

- Aunque sean utilizados medios de protección para tener la información segura, no puede asegurarse completamente que estos no serán comprometidos; pero aplicando una serie de políticas es posible generar una capa de protección adicional, que permita la prevención y mitigación de algunas amenazas, y haga al entorno informático más seguro.

- El factor humano no es tomado en cuenta en las compañías, aunque este juega un papel fundamental en la seguridad, debido a que son los usuarios, los que de manera constante interactúan con los sistemas, y los Ciberdelincuentes orientan sus ataques en la falta de conocimiento de ellos. Por tal motivo es fundamental realizar capacitaciones periódicas sobre cómo ayudar a prevenir ataques cibernéticos

- Según las estadísticas mostradas en los últimos informes de variantes de Ransomware, este tipo de amenazas continuaran estando presentes en el ecosistema de tecnología en los siguientes años, proteger la red corporativa mediante elementos de seguridad perimetral aumentara la protección frente a esas amenazas que son constantes por el simple hecho de necesitar usar la red pública , aplicando la protección de manera más granular ,los dispositivos que

usan los usuarios para sus tareas cotidianas como equipos de escritorio y laptops , deben tener su propio mecanismo de defensa , antivirus y firewall son algunos de estos elementos. Un elemento esencial a la hora de hacer frente al Ransomware es un buen sistema de sistema de backup, dado el caso alguna de las capas de protección mencionadas anteriormente fallará en la contención del virus, la copia de seguridad devolverá la integridad de los datos y la disponibilidad del servicio que presta la Compañía podrá continuar.

RECOMENDACIONES

- ✓ Que los usuarios puedan utilizar equipos portátiles para realizar las tareas que deben hacer en sus empresas, es una gran ventaja pues les da una gran flexibilidad para cumplir sus objetivos. El hecho de que el equipo salga de la red corporativa da pie a que pierda una capa de protección que brinda la red interna. A continuación, se da una serie de recomendaciones para reducir estos riesgos asociados a la movilidad.

  - Restricciones para software y recursos: ya que estos dispositivos tendrán información valiosa de la empresa, una buena práctica será el cifrado de la información, de esta forma se evitará que si el dispositivo cae en las manos incorrectas la confidencialidad de la información no se vea comprometida, también programas que no hagan parte del uso corporativo deberán ser restringidos para evitar fuga de información y mal uso de los dispositivos en otro tipo de actividades.

  - Clasificar Datos: al ser dispositivos que los usuarios usaran tanto en la compañía como en sus hogares, estos se pueden llenar de datos personales que el usuario haya guardado, por esta razón es necesario tener una

política definida de clasificación de datos para que el equipo cuando entre a la compañía no exponga los datos personales del usuario y conserve su privacidad

- Copia de seguridad: Tanto si el dispositivo permanece dentro de las instalaciones como si no, la copia de seguridad de este y de sus datos debe ser garantizada, existen herramientas basadas en Cloud, donde a través de agentes se puede hacer la copia de seguridad y que los respaldos sean guardados en la nube.

- Seguridad Endpoint: existen herramientas de seguridad en el mercado que utilizan Agentes y diferentes módulos de seguridad para dar protección a dispositivos portátiles, una vez estos salen de la red corporativa, entre estos están firewall a nivel de host, protección web a nivel de host y antivirus corporativos. Las políticas a estos dispositivos son establecidas en la red Interna y aplicadas a los equipos, cuando uno de estos equipos abandona la red, estas políticas se conservan, luego una vez el dispositivo vuelve a la red, las políticas serán actualizadas en caso de que estas hayan cambiado.

✓ Es de gran importancia definir planes de acción documentados, para tener una respuesta adecuada, antes de que ocurra un evento que comprometa la seguridad de la información de la organización. De esta manera se simplificará la reacción frente a la interrupción de alguno de los servicios críticos de la empresa y volverán a estar en marcha lo más pronto posible.

- ✓ Es fundamental que la organización cuente con un plan de acciones de prevención, diagnóstico y solución; claro, concreto y documentado, pues de esta manera se puede dar continuidad al negocio con el menor impacto negativo posible.

- ✓ Hacer un análisis de riesgo para definir los elementos que deben ser protegidos en las compañías.

TRABAJO FUTURO

- La realización del trabajo de grado fue basada en la protección frente a amenazas Ransomware desde 3 frentes la seguridad perimetral, la seguridad a nivel de host y la Copia de seguridad. Algunos de los enfoques o trabajos futuros que podrían complementar el trabajo de grado son los siguientes:

    - Realizar la integración y configuración de un dispositivo Sandbox para el control de amenazas informáticas en un entorno seguro, antes de que puedan hacer daño ingresando a la red corporativa, se pueden analizar diferentes fabricantes de este tipo de dispositivos y usar una versión de prueba virtualizada para su estudio.

    - Validar la conveniencia, las ventajas y desventajas de la utilización de un dispositivo SIEM (Security Information and Event Management) en la red corporativa, realizar una descripción de sus características y sus configuraciones básicas.

6. REFERENCIAS

Budd, C. (9 de 9 de 2016). *blog trendmicro*. Obtenido de http://blog.trendmicro.com/outsourcing-crime-how-Ransomware-as-a-service-works/

Damoulakis, J. (11 de 2005). *techtarget*. Obtenido de http://searchdatabackup.techtarget.com: http://searchdatabackup.techtarget.com/tip/Best-practices-10-basic-steps-for-better-backup

Elovici, & Rokach. (2014). *Reaction to New Security Threat Class.* Israel: Cornell University Library.

Garcia, D. F. (Junio de 2014). *TESIS DE GRADO.* Obtenido de puce.edu.ec: http://repositorio.puce.edu.ec/bitstream/handle/22000/7896/9.56.000616.pdf?sequence=4&isAllowed=y

Kevin Savage, P. C. (2015). The evolution of Ransomware. *Security Response ,Symantec*, 57.

labs, m. (2016). *mcafee labs.* Obtenido de www.intelsecurity.com

Liao, Q. (s.f.). A GROWING THREAT TO SMES. *A GROWING THREAT TO SMES*. TEXAS, USA: The University of Texas at Brownsville and Texas Southmost College.

Mcafee Labs. (2016). *McAfee Labs Threats Report.* California.

McAfee Labs. (2017). *McAfee Labs Threats Report.* Madrid.

Medina, E. (11 de 2016). *Muy Seguridad*. Obtenido de Muy Seguridad: http://muyseguridad.net/2016/10/11/detectar-5-senuelos-phishing-email/

Ramos, M. d. (2011). *Seguridad Informatica.* Madrid: Ediciones paraninfo.

Rouse, M. (07 de 2013). *Techtarget.* Obtenido de Techtarget: http://whatis.techtarget.com/definition/endpoint-device

Rouse, M. (12 de 2016). *techtarget.* Obtenido de http://searchdatacenter.techtarget.com/es/definicion/Red-de-area-local-LAN

Santos, J. C. (2011). *Seguridad Informatica.* Bogotá: Ediciones de laU.

Technology, N. I. (12 de 02 de 2014). *National Institute of Standards and Technology.* Obtenido de https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Techtarget. (1 de Abril de 2016). *¿Qué software de protección de punto final es en su lista?* Obtenido de SearchSecurity.com: http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=115271530&lang=es&site=ehost-live

Trend Micro. (11 de 08 de 2017). Obtenido de https://www.trendmicro.com: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/best-practices-Ransomware

FIRMA ESTUDIANTES _____

_____

FIRMA ASESOR _____

FECHA ENTREGA: _____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

_____

RECHAZADO_ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____