FACULTAD DE INGENIERIA DE CIENCIAS AGROPECUARIAS

.

EVALUACIÓN DE POSIBLES VULNERABILIDADES/AUDITORÍA DE SEGURIDAD Y PROPUESTA DE MEDIDAS DE MITIGACIÓN DENTRO DE LA RED INTERNA JUNTA NACIONAL DE DEFENSA DEL ARTESANO.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Tecnólogo en Redes y Telecomunicaciones

Profesora Guía

Ing. Mery Elizabeth González Tello

Autor

Darwin Marcelo Folleco Gonzalón

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Ing. Mery Elizabeth González Tello

1715149298

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Ing. Fabian Wladimiro Basantes Moreno.

1709767667

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Darwin Marcelo Folleco Gonzalón

1724810476

AGRADECIMIENTOS

A Dios todo poderoso, porque su tiempo es perfecto, a mi familia por el apoyo brindado en este camino, a mis hijas que son mi mayor motivación y, a mi profesor guía por su tiempo y dedicación.

DEDICATORIA

A mi madre, motor fundamental en mi crecimiento y supo inculcar en mí, valores esenciales para mi crecimiento. A mi padre por su constancia y apoyo y, a las personas más importantes en mi vida, Josianny y Geraldine, mis hijas, que son mi motivación para seguir creciendo profesionalmente y como persona de bien.

RESUMEN

El presente trabajo, comprende la evaluación de vulnerabilidades que tiene la red informática de la Junta Nacional de Defensa del Artesano, esto ante posibles ataques informáticos, mismos que pueden manifestarse de diferente manera según la necesidad del atacante.

La seguridad informática es la base sólida que se debe tener en un esquema de una red LAN, ya que de ello depende el correcto funcionamiento de la misma y permite la optimización de recursos, tanto interna como externamente.

La propuesta de medidas de mitigación y la implementación de la mismas, dan como resultado una red más segura, con la capacidad de prevenir posibles ataques informáticos; la falta de políticas de seguridad y ausencia de control pueden derivar en problemas como pérdida del control de la red, fuga de información confidencial, sobrecarga en los recursos como ancho de banda, etc.

ABSTRACT

The present work includes the evaluation of vulnerabilities that the Junta Nacional de Defensa del Artesano has in its computer network, which can manifest in different ways according to the need of the attacker.

The computer security is the solid base that must be had in a scheme of a LAN network.

The proposal of mitigation measures and the implementation of the same, result in a more secure network, with the capacity to prevent possible computer attacks; The lack of security policies and lack of control can lead to problems such as loss of control of the network, leakage of confidential information, overloading of resources such as bandwidth, etc.

ÍNDICE

Índice de Figuras

Índice de Tablas

INTRODUCCIÓN.

La Junta Nacional de Defensa del Artesano tiene la misión de liderar el fortalecimiento, profesionalización y desarrollo de todo el sector artesanal que produce bienes y servicios, mediante el impulso de una política pública, la formación, la investigación y la prestación de servicios a los artesanos y artesanas.

Actualmente la Junta Nacional de Defensa del Artesano ubicada en la calle Mariscal Foch E4- 38 entre Av. Colón y Cordero, cuenta con alrededor de 100 equipos informáticos conectados entre sí a través de redes LAN y W-LAN, tales como servidores, computadores, impresoras y dispositivos móviles, mismos que podrían ser víctimas de cualquier tipo de ataques.

El objetivo de realizar una propuesta de medidas de mitigación, para la red interna de la Junta Nacional de Defensa del Artesano, es con propósito de proteger la misma; por motivo de tratarse de una entidad de derecho público, maneja información confidencial e importante de sus registros artesanales, tales como: Nombres completos, números de cédula, direcciones domiciliarias y de talleres artesanales, capitales invertidos, entre otras. Esta información se la debe llevar con la mayor de las responsabilidades y la misma esta almacenada en servidores y computadores institucionales, por ende, para que esté completamente segura, se ha propuesto este tema, como medida de protección de información mediante la seguridad informática.

CAPITULO I - Evaluación de vulnerabilidades que tiene una red interna.

1.1 Concepto de Seguridad de Redes.

Según (Tanenbaum, 2012), las seguridades de las redes se pueden dividir en cuatro (4) áreas que están relacionadas entre sí, estas son: confidencialidad, autenticación, no repudio y control de integridad; donde, la confidencialidad se encarga de mantener datos fuera del alcance de usuarios no autorizados. La autenticación consiste en determinar a quién va dirigida la información, antes de ser revelada o hacer un trato de negocios. El no repudio, es aquel que se encarga de las firmas, esto quiere decir que realice el trámite de comprobación de solicitud. El control de integridad tiene que ver con la forma en que podemos estar seguros de que el mensaje o información recibido, fue el que realmente se envió y no algo que un adversario malicioso modificó en el camino.

La seguridad de red es la actividad que mantiene “vivo” el estado de seguridad, esto quiere decir que supervisa, audita y diseña las acciones y procesos de mejoras necesarias para mantener el ciclo. (Estrada, 2016)

Todos los usuarios de informática, que pertenecen o presten sus servicios a entidades públicas o privadas, tienen en gran parte expectaciones informales respecto a los computadores: esperan que al presionar el botón de encendido el computador guarde todos los datos tal y como los dejaron antes de apagarlos; cuando envían un mensaje de correo electrónico, esperan que llegue a su receptor en un lapso razonable sin perder ninguno dato; cuando ingresan a la base de datos de nóminas, esperan que los sueldos y los nombres de los empleados sean los auténticos y no hayan cambiado. En definitiva, los usuarios albergan gran cantidad de expectativas que, por desgracia, no siempre se verán cumplidas: un fallo de hardware podría hacer perder los datos del disco; el mensaje de correo junto con su archivo adjunto podría ser interceptado por un intruso; un empleado desleal con excesivos privilegios de acceso podría

manipular la aplicación de nóminas. Si no se toma ninguna medida de protección, la mayoría de expectativas respecto a la informática se verán defraudadas, por motivo de que la información está expuesta a innumerables amenazas, cada una con una probabilidad de ocurrencia y un riesgo asociado: hackers externos, virus, gusanos, troyanos, empleados descontentos o sobornados, fallos de hardware o de software, interrupciones en el suministro eléctrico, fuegos, incendios e inundaciones, la lista sería interminable. La seguridad informática es el método que se ocupa de administrar el riesgo dentro de los sistemas informáticos. Dicho de otra manera, mediante la aplicación de estos principios, se establecerán en los sistemas informáticos las medidas de seguridad capaces de neutralizar las amenazas a las que se encuentran expuestos los dispositivos institucionales: la información y los elementos hardware y software que la soportan. No se trata de implantar a la ligera medida de seguridad, tales como cortafuegos o cifrado de datos porque tal o cual tecnología está de moda o porque se cree que se así se tendrá un sistema más seguro. Se trata más bien de evaluar los riesgos reales a los que la información está expuesta y mitigarlos mediante la aplicación de las medidas necesarias y en el grado adecuado, con el fin de satisfacer las expectativas de seguridad generadas. (Álvarez Marañón & Pérez García, 2004)

1.2 Tipos de Ataque.

Los sistemas informáticos, puedes ser vulnerados por diferentes tipos de ataques, cada uno de ellos pueden tener diferentes propósitos.

Según (Roa Buendía, 2013), los ataques más comunes son:

- Interrupción.
- Interceptación.
- Modificación.
- Fabricación.
- Ingeniería Social.

- Pishing.
- Keyloggers.
- Fuerza Bruta.
- Sniffing.
- DoS.
- DDoS.

1.2.1 Interrupción.

Este ataque se encarga de inducir una interrupción en la presentación de un servicio: la presentación web no está disponible, la presentación en la red no está disponible.

1.2.2 Interceptación de servicio.

Es cuando el atacante ha conseguido ingresar a un sistema comunicacional y ha logrado copiar la información que se estaba transmitiendo.

1.2.3 Modificación.

Es cuando el atacante ha logrado ingresar, pero su objetivo no es copiar la información interceptada, sino modificarla para que esta llegue modificada hasta su destino final y provoque confusión al usuario.

1.2.4 Fabricación.

Es cuando el atacante toma la forma, o se hace pasar por el destinatario de la trasmisión, por lo que en este punto puede tranquilamente conocer el objeto de nuestra comunicación.

1.2.5 Ingeniería Social.

A la hora de fijar una contraseña, el usuario suele utilizar combinaciones relacionadas a su vida cotidiana (fecha de cumpleaños, nombres especiales, etc.).

Puede constituir también al momento de pedir un favor a algún compañero de trabajo, tal como introducir su contraseña, que el de usuario parece que no funciona,

1.2.6 Pishing.

Consiste en que el atacante se pone en contacto con la víctima, generalmente por correo electrónico y se hace pasar por una empresa con la que tenga alguna relación. En el contenido del mensaje intentará convencer para que la víctima haga clic sobre un enlace que lo llevará a una falsa web de la empresa. En esa web solicitarán su identificación habitual y desde ese momento el atacante podrá utilizarla.

1.2.7 Keyloggers.

Se trata de un troyano que puede tomar nota de todas las teclas que presionamos en algún formulario determinado que sea de interés del atacante.

1.2.8 Fuerza Bruta.

Se trata del tipo de ataque en el cual el atacante puede ir generando combinaciones aleatorias, con el objetivo de poder descifrar una contraseña.

1.2.9 Spoofing.

Este tipo de ataque altera un dispositivo de la máquina para hacerse pasar por otra máquina. Por ejemplo, generar recados con la misma dirección que la máquina legitima.

1.2.10 Sniffing.

Es cuando el atacante consigue enlazarse en el mismo tramo de red que el equipo atacado. De esta forma tiene acceso directo a todas sus conversaciones.

1.2.11 DoS.

(Denieal of Servise, denegación de servicio). Consiste en derribar un servicio, llenándolo con falsas peticiones de conexión. Es decir, intenta fingir la consecuencia de una carga de trabajo varias veces superior a la normal.

1.2.12 DDoS.

(Distributed Denial of Service, denegación de servicios distribuida). Es igual al ataque DoS, pero ahora no es una máquina única la que crea las solicitudes aparentes o falsas (que es fácilmente localizable y permite actuar contra ella), sino muchas máquinas dispersas por distintos puntos del planeta, Esto es posible porque todas esas máquinas han sido infectadas por un troyano que las ha convertido en ordenadores zombis (obedecen las órdenes del atacante).

1.3 Virus.

Un virus es un programa que puede con el normal funcionamiento de otros programas; la modificación de estos programas, por lo general incluye una copia del programa de virus, que, con el tiempo, puede continuar infectando y atacando a otras aplicaciones instaladas

Los virus, se los puede definir cómo extracto de código genético que pueden llegar a controlar una máquina de una célula viva y transformarla en millones de réplicas similares al virus original. (Stallings, 2004)

1.3.1 Fases de Virus.

Según (Stallings, 2004), el virus, durante su desarrollo, pasa por cuatro diferentes períodos o etapas, estas son:

- Fase Iniciativa.
- Fase de Prolongación.
- Fase de Activación.
- Fase de Ejecución.

1.3.1.1 Fase Iniciativa.

El virus está en estado de inactividad, pero al final, terminará cambiando su estado a activo por algún suceso, como una fecha, actividad de algún programa o archivo, o la exuberancia de uso de la capacidad por parte de un disco.

1.3.1.2 Fase de Prolongación.

El virus se encarga de poner una réplica exacta de si mismo en otros programas o en determinadas áreas de un disco. Cada sector que sea infectado contendrá desde el momento del ataque, un clon del virus, que a su vez entrará en fase de propagación o prolongación.

1.3.1.3 Fase de Activación.

El virus se activa para llevar a cabo la función para la cual se creó. Al igual que en la fase inactiva, la fase de activación puede ser producida por una variedad de acontecimientos en el sistema, incluyendo un cálculo del número de veces que esta copia del virus ha hecho copias de sí mismo.

1.3.1.4 Fase de Ejecución.

El virus llega a la función de ejecución y al parecer puede ser inofensiva, manifestándose como un simple mensaje en pantalla, o puede ser tan perjudicial como la de pérdida de archivos y programas importantes.

La gran mayoría de los virus, realizan su labor de manera específica, como por ejemplo para atacar un sistema operativo, o en otros casos para destinar su ataque a una plataforma de hardware.

1.3.2 Tipos de virus.

En relación a los tipos de virus, (Stallings, 2004), los ha clasificado detallado de la siguiente manera:

- Virus Parásito.
- Virus Residente en la Memoria.
- Virus del Sector de Arranque.

- Virus Furtivo.
- Virus Polimórfico.

1.3.2.1 Virus Parásito.

Es el típico virus y hoy en día el más común. Este tipo de virus se caracteriza por adjuntarse por si mismo a los archivos ejecutables y se va repitiendo cuando el archivo infectado se ejecuta, de esta manera va encontrando otros programas que pueden ser infectados.

1.3.2.2 Virus Residente en la Memoria.

Tiene como objetivo, alojarse en la memoria principal del equipo, haciéndose pasar como parte de un archivo.

1.3.2.3 Virus del Sector de Arranque.

Este tipo de virus ataca principalmente al sistema de arranque y se va extendiendo cuando el registro de arranque de sistema es ejecutado.

1.3.2.4 Virus de tipo Furtivo.

Es un virus delineado específicamente para no ser detectado por el antivirus

1.3.2.5 Virus Polimórfico.

Es el tipo de virus que se encarga de crear copias de si mismo durante ejecuciones fundamentales, pero que tienen a simple vista diferentes parámetros de bits. De la misma manera que el virus furtivo, el objetivo es no ser visible para los antivirus.

1.4 Tipos de Atacante.

(Roa Buendía, 2013), afirma que se puede denominar como hacker a aquel individuo, que, mediante procesos o conocimientos adquiridos, puede saltarse cualquier tipo de protección de un sistema, por lo que se los puede clasificar de la siguiente manera:

- Hacker.
- Cracker.
- Script Kiddie.
- Programadores de malware.
- Sniffers.
- Ciberterroristas.

1.4.1 Hacker.

Es aquel que puede vulnerar la seguridad informática de un sistema, solo por el reto que presume hacerlo. Si logra su objetivo, moralmente informará a los administradores de la red, sobre los agujeros de seguridad que ha empleado para lograr su propósito.

1.4.2 Cracker.

Su objetivo principal, aparte de vulnerar la defensa, es el de hacer daño mediante desactivaciones de servicio, alteración de información, robo de datos, etc.

1.4.3 Script Kiddie.

Son principiantes de hacker y craker, que, por curiosidad, puede encontrar cualquier tipo de ataque en internet y lo lanzan sin saber muy bien las consecuencias de sus actos y, sobre todo, las consecuencias terminales de sus actuaciones (este hecho los convierte en potencialmente peligrosos).

1.4.4 Programadores de malware.

Se trata de individuos con altos conocimientos en programación de sistemas operativos y en aplicaciones, capaces de aprovechar vulnerabilidades de alguna versión desarrollada de un software común para generar aplicaciones que lo puedan atacar.

1.4.5 Sniffers.

Son expertos en protocolos comunicacionales y son capaces de procesar capturas de tráfico de red para interactuar con información relevante.

1.4.6 Ciberterroristas.

Cracker o individuos con fines de interés económicos y políticos a gran escala.

1.5 Métodos de Protección.

Siempre se debe tomar en cuenta que lo primordial en una red informática es la seguridad, ya que de ella dependerá la privacidad de la información y que la misma esté libre de riesgo de posibles atacantes, para ello es necesario la implementación de políticas de seguridad como parte fundamental y de sistemas (hardware y software), o métodos de protección, que puedan trabajar dentro de la red, con el fin de proveer el servicio de seguridad necesario.

Existen varios métodos de protección, de entre los más utilizados se puede mencionar los siguientes:

- Intrusion Detection System (IDS)
- Web Application Firewall (WAF)
- Cortafuegos (firewall)
- Antivirus
- Proxy
- Router Filtrado

1.5.1 Intrusion Detection System (IDS).

Según (Larrieu, 2003), el término IDS (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existe dos familias de IDS, las cuales son:

- N-IDS (Sistema de detección de intrusiones de red).
- H-IDS (Sistema de detección de intrusiones en el host).

1.5.1.1 N-IDS (Sistema de detección de intrusiones de red).

Un N-IDS necesariamente depende de un hardware exclusivo. Éste arma un sistema capaz de verificar paquetes de información que se transportan por una o más vías de la red para identificar si se ha producido alguna actividad maliciosa. El N-IDS coloca uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. (Larrieu, 2003)

1.5.1.2 H-IDS (Sistema de detección de intrusiones en el host).

El H-IDS se encuentra en un host particular. Por lo tanto, su software cubre una amplia gama de sistemas operativos como Windows, Solaris, Linux, HP-UX, Aix, etc.

El H-IDS actúa como un daemon o servicio estándar en el sistema de un host. Tradicionalmente, el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer). (Larrieu, 2003)

1.5.2 Web Application Firewall (WAF).

Los WAF son un tipo de firewall que se utilizan para controlar el acceso a una aplicación o servicio web. A diferencia de un *firewall* tradicional, un IPS o IDS, la ventaja de un WAF es que opera sobre la capa de aplicación (capa 7 del modelo OSI), por lo que es posible considerar algunos tipos de protecciones más allá de las tradicionales con los dispositivos mencionados.

Durante el desarrollo de una aplicación web suelen detectarse vulnerabilidades. Muchas de ellas residen sobre alguna funcionalidad en particular. Según la criticidad del caso, en algunas circunstancias no es posible mitigarlas de forma inmediata debido a que requiere rediseñar la propia aplicación. En otros casos, la criticidad de la información y las tareas que realiza la aplicación web no permite realizar los cambios necesarios para mitigar las vulnerabilidades detectadas.

En esta instancia, se suele utilizar un WAF. De esta manera, es posible configurar la regla necesaria para que la vulnerabilidad no pueda ser

explotada. Esto permite solventarlas hasta que se solucione a nivel de diseño. (CATOIRA, 2013)

1.5.3 Cortafuegos (firewall).

Según (Dordoigne, 2015), un equipo cortafuego (firewall), se encarga de convertir las múltiples redes accesibles y conectables, en independientes.

Los nuevos cortafuegos, llamados también de aplicación, son capaces de analizar algunos segmentos de paquetes, como los de los protocolos HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), etc. Este rango de análisis permite disminuir las nuevas maneras de ataque, que se valen de los fallos de las aplicaciones comunes.

El cortafuego de borde comúnmente va acompañado de un firewall personal, que va instalado en los equipos de trabajo. Así, los computadores se resguardan de ataques que podrían provenir desde la red local; en la figura 1, se puede observar el diagrama de funcionamiento de firewall.

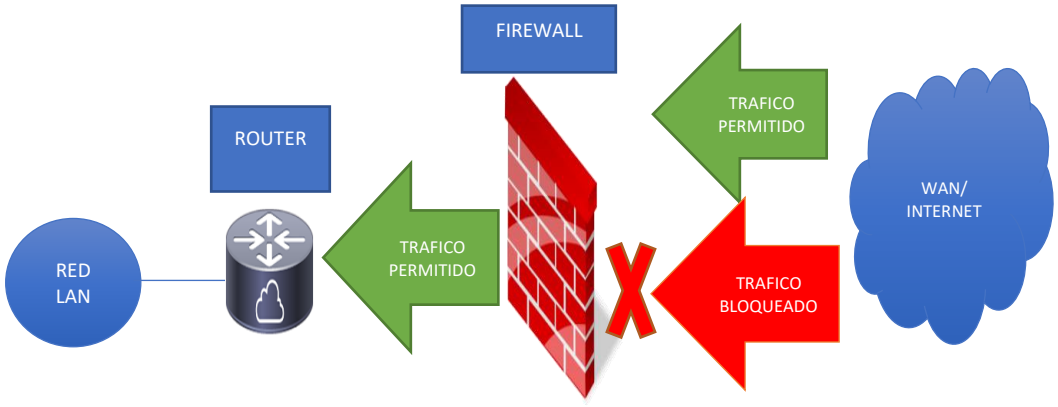


Figura 1. Diagrama de Funcionamiento de Firewall.

Según (Roa Buendía, 2013), el cortafuego es un sistema que interfiere entre el software y las aplicaciones de red para hacer un filtrado de paquetes:

- En el tráfico que ingresa, la tarjeta de red recibe los paquetes y los identifica, no sin antes pasar por el filtro de firewall, quien decidirá si estos son aptos o no para ingresar.
- En el tráfico de salida, las aplicaciones obtienen sus paquetes de datos, pero antes, pasa por el firewall para que pueda ser enviado a una red.

El firewall actúa generalmente en las máquinas servidor por el tráfico de red entrante: los valores que ejecutan dentro de este equipo abren determinados puertos previamente configurados. En las máquinas cliente, el proceso es mucho más sencillo; por defecto, todas las conexiones no están habilitadas y todas las salientes habilitadas. Esto no significa que no puedan ingresar paquetes, porque no habría diálogos; pero los diálogos los tiene que iniciar el equipo cliente. (Roa Buendía, 2013)

El talento del firewall se manifiesta mediante reglas de configuración. El administrador del equipo puede activarlas, desactivarlas, modificarlas o añadir nuevas, siempre y cuando tenga los permisos suficientes para realizar esta acción. (Roa Buendía, 2013)

Las reglas un cortafuego son mucho menos complicadas que las reglas de un IPS (sistema de prevención de intrusos) y comúnmente solo se emplean las cabeceras TCP/IP de las capas 3 (red) y 4 (trasporte). (Roa Buendía, 2013)

1.5.4 Antivirus.

El antivirus es un software que está controlando de manera continua lo que ocurre en los equipos. Resumidamente, cualquier software que intenta

ejecutarse (ejecutables .exe, librerías .dll) debe primero pasar por el antivirus. Este lo compara con su base de datos de virus y, si lo encuentra, niega su ejecución y alerta al usuario. (Roa Buendía, 2013)

El antivirus es una aplicación de software que ha sido diseñada como alternativa de protección y seguridad para proteger los datos y sistemas informáticos de aplicaciones conocidas comúnmente como virus que tienen el fin de alterar, perturbar o destruir el correcto desempeño de las computadoras.

Un antivirus tiene la funcionalidad común que en general compara el código de cada archivo que revisa con una base de datos de virus ya conocidos y, de esta manera, puede establecer si se trata de un componente dañino para el sistema. También puede identificar una actuación o conducta típica de un virus. Los antivirus pueden analizar tanto los archivos que se encuentran dentro del sistema como aquellos que buscan ingresar o interactuar con el mismo.

A medida que nuevos virus se van creando constantemente, siempre es necesario mantener actualizado el antivirus, de tal manera que se pueda reconocer a las nuevas versiones maliciosas. Así, el antivirus puede mantenerse en ejecución durante todo el tiempo que el sistema permanezca encendido, o bien, registrar un archivo o serie de archivos cada vez que el usuario lo requiera. Un antivirus puede complementarse con otros sistemas de seguridad como firewalls que cumplen funciones adicionales para evitar el ingreso de virus. (Bembibre, 2008)

1.5.5 Proxy.

Según (Dordoigne, 2015), el servidor proxy es utilizado principalmente en el perímetro del tráfico HTTP (Hyper Text Transfer Protocol), o inclusive con FTP (File Transfer Protocol), en la red LAN (Local Area Network) e Internet.

Cuando obstaculiza una petición hacia una red externa, el proxy la redirige como si fuera de su propiedad y a continuación, guarda los datos recibidos. Seguidamente, los remite al peticionario inicial. El sistema Proxi es interesante por camuflar las direcciones IP internas, puesto que la solicitud no llega a Internet. Y luego permite prohibir el acceso a algunos sitios Web. (Dordoigne, 2015)

Otra ventaja del servidor proxy es su capacidad para disponer una memoria caché. Así, es posible volver a solicitar un archivo o un sitio web. (Dordoigne, 2015)

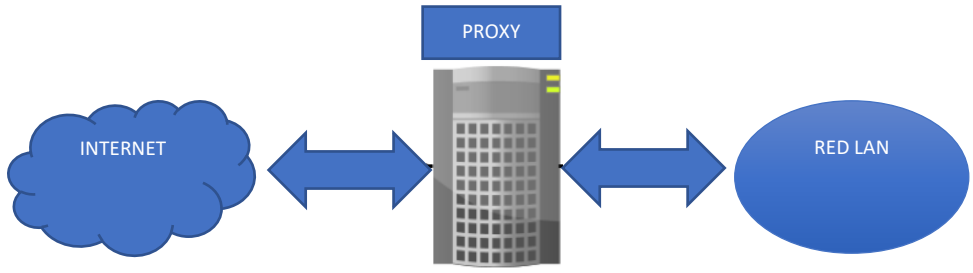


Figura 2. Diagrama de Funcionamiento de Proxy.

Según (Roa Buendía, 2013), Un servidor proxy es un servicio de red que hace de mediador en un determinado protocolo. El servidor proxy más común es el proxy HTTP: un navegador en un computador cliente que requiere descargar una página web de un servidor no lo hace directamente, sino que solicita a un servidor proxy que lo haga por él.

El proceso del servidor proxy se puede llevar a tomar la decisión de no generar ningún mensaje. Esto quiere decir, negar la comunicación. Este proceder se decide mediante reglas. En estas reglas se puede filtrar determinadas direcciones de origen o destino, algunas directivas del protocolo, inclusive contenido multimedia. Como se puede suponer, cuanto más complicada sea la

regla, más tardará el proxy en aplicarla a las peticiones que le llegan, lo que puede ralentizar en exceso la comunicación. (Roa Buendía, 2013)

1.5.5.1 Tipos de Proxy.

Según (Roa Buendía, 2013), se puede clasificar a los servidores Proxy de la siguiente manera:

- **Proxy explícito. –** Se configura en los navegadores de los usuarios para que puedan utilizar el proxy de la empresa.

- **Proxy transparente. –** Se configura en algún punto de la red, donde el router filtrará todo tipo de tráfico y procederá a enviárselo al proxy sin que el usuario tenga que hacer nada.

1.5.6 Router Filtrado.

(Dordoigne, 2015) afirma que, los dispositivos de filtrado que se pueden relacionar a un router admiten el análisis de la capa 3 del modelo OSI.

La revisión de los paquetes que entran y salen se efectúa, en la cabecera IP, lo que aprueba acciones como:

- Bloqueo total de direcciones IP (origen y destino).
- Prohibición de transmisión de datos

Algunos computadores contienen las cabeceras de capa 4 del modelo OSI. Así se puede realizar un filtrado en los puertos TCP o UDP e inclusive realizar la revisión de datos de aplicación.

CAPITULO II: Análisis y auditoría de las posibles vulnerabilidades que tiene la red interna de la Junta Nacional de Defensa del Artesano.

La red interna de la Junta Nacional de Defensa del Artesano cuenta con diversos equipos informáticos, entre estos están: ordenadores móviles, estaciones de trabajo fijas, servidores, etc., los mismos que se detallan a continuación, según sus características.

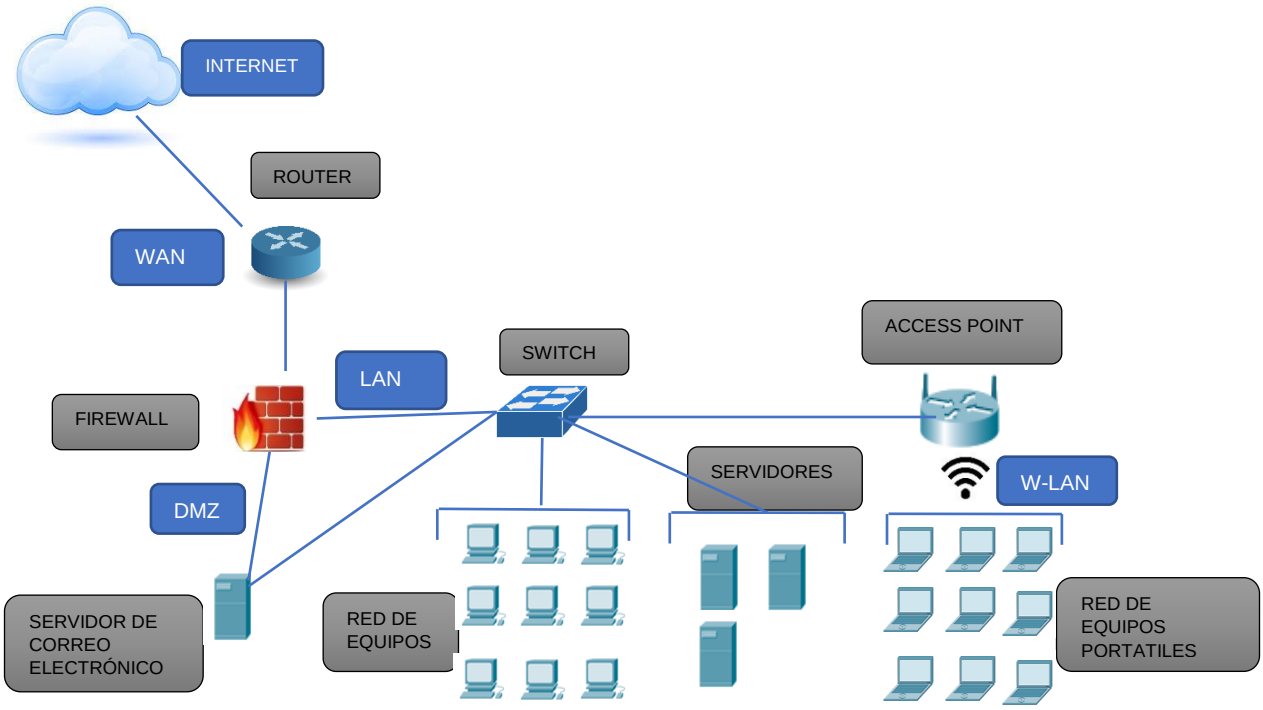


Figura 3. Esquema de Mapa de red JNDA

Red de Servidores – El direccionamiento de IPs para los equipos servidores van desde la dirección xxx.xxx.xx.03 hasta la dirección xxx.xxx.xx.20.

Tabla 1.

Distribución de Servidores de la JNDA

Tipo de Servidor	**Sistema Operativo**	**Características**	**Servicio**
Físico	Microsoft Windows Server 2003 R2	1.00 GB Ram	Servidor de aplicativos
Físico	Microsoft Windows Server 2003 R2	Intel® Xeon® CPU E5310 1.60Ghz 1.60 Ghz 2.00GB de Ram	Servidor software contable y registro artesanal
Físico	PFSENSE, basado en software libre	Intel® Core™ i5-2400 CPU @ 3.10GHz.	Servidor de Firewall

Red de Usuarios – El direccionamiento de IPs para los equipos de usuario van desde la dirección xxx.xxx.xx.21 hasta la dirección xxx.xxx.xx.200.

Tabla 2.

Distribución de equipos de usuario

Cantidad	**Tipo**	**Sistema operativo**
60	Computadores de escritorio	Microsoft Windows 7 PRO
4	Computadores portátiles	Microsoft Windows 8.1
4	Computadores portátiles	Microsoft Windows 10

2.1 Seguridad actual dentro de la red interna de la Junta Nacional de Defensa del Artesano.

Actualmente la red interna de la Junta Nacional de Defensa del Artesano cuenta con niveles de seguridad básicos, los cuales constan de un firewall perimetral de código abierto (PFSENSE) el cual se encarga de regular las conexiones entrantes y salientes desde y hacia la red, actualmente esa instalado en uno de los servidores y su administración se la realiza mediante Web Service.

De igual manera, cuenta con sistema de antivirus licenciado(ESET), mismo que se encarga de la seguridad a nivel de usuario, este se lo administra de igual manera desde un servidor web y, los clientes están instalados en cada uno de los computadores que son usados por los funcionarios.

2.1.1 Firewall PFSENSE.

El proyecto pfSense es una distribución de firewall de red libre, basada en el sistema operativo FreeBSD con un kernel personalizado e incluye paquetes de software libre de terceros para funcionalidad adicional. El software pfSense, con la ayuda del sistema de paquetes, puede proporcionar la misma funcionalidad o más de firewalls comerciales comunes, sin ninguna limitación. Ha reemplazado con éxito todos los cortafuegos comerciales de gran nombre. (PFSENSE, 2017)

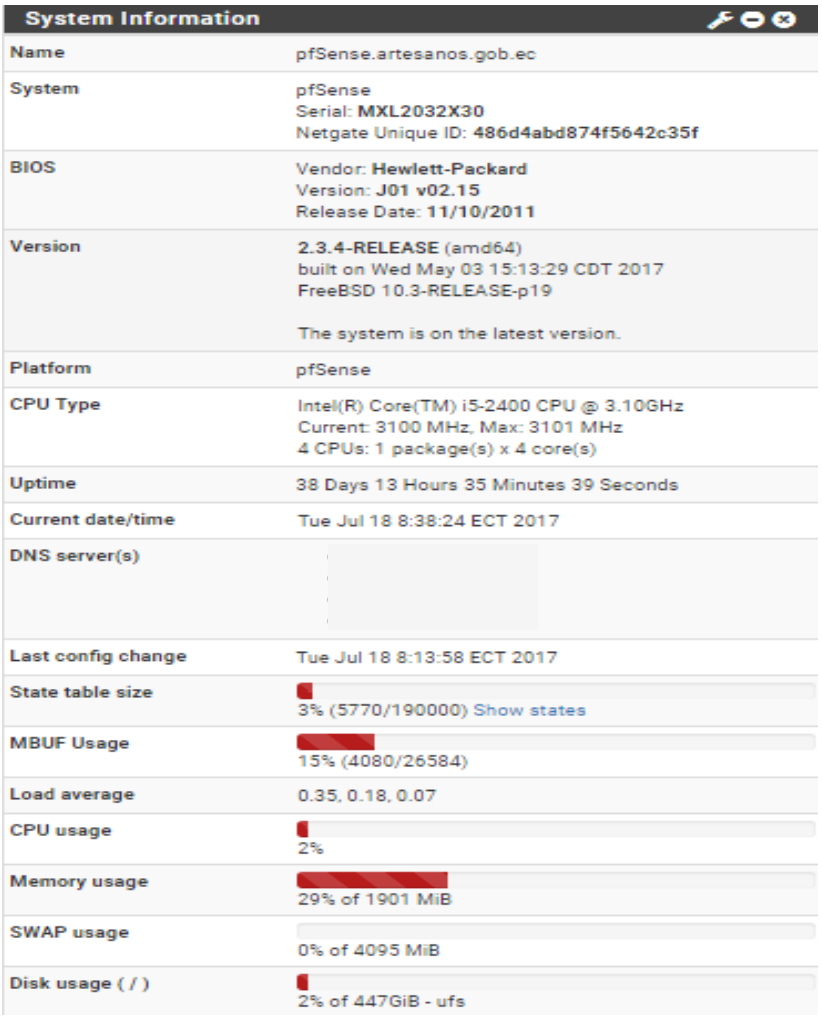
2.1.1.1 Administración PFSENSE.

La administración del firewall PFSENSE, se lo realiza mediante Web Service; para dicho proceso, se tiene que ingresar mediante cualquier navegador a la siguiente dirección: https://xxx.xxx.xx.5:40443/index.php (por políticas de seguridad, este proceso se lo puede realizar solo desde un computador o dispositivo que esté conectado directamente a la red de la JNDA), como se observa en la figura 3.

Figura 4. Captura pantalla Login PFSENSE JNDA.
Tomado de https://192.xxx.x.x:40443

Una vez ingresadas las credenciales, la interface nos redirigirá directamente a la pantalla de dashboard, en donde se podrá visualizar las estadísticas, el estado, las interfaces configuradas, la información del sistema, etc.

En la sección de System Information, se puede visualizar datos referentes al hardware donde está instalado el firewall, entre se puede encontrar información como: nombre, modelo del sistema, BIOS, versión, plataforma, tipo de cpu. Fecha de entrada a funcionamiento, entre otras; tal como se visualiza en la figura 4.



System Information	
Name	pfSense.artesanos.gob.ec
System	pfSense Serial: **MXL2032X30** Netgate Unique ID: **486d4abd874f5642c35f**
BIOS	Vendor: **Hewlett-Packard** Version: **J01 v02.15** Release Date: **11/10/2011**
Version	**2.3.4-RELEASE** (amd64) built on Wed May 03 15:13:29 CDT 2017 FreeBSD 10.3-RELEASE-p19 The system is on the latest version.
Platform	pfSense
CPU Type	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz Current: 3100 MHz, Max: 3101 MHz 4 CPUs: 1 package(s) x 4 core(s)
Uptime	38 Days 13 Hours 35 Minutes 39 Seconds
Current date/time	Tue Jul 18 8:38:24 ECT 2017
DNS server(s)	
Last config change	Tue Jul 18 8:13:58 ECT 2017
State table size	3% (5770/190000) Show states
MBUF Usage	15% (4080/26584)
Load average	0.35, 0.18, 0.07
CPU usage	2%
Memory usage	29% of 1901 MiB
SWAP usage	0% of 4095 MiB
Disk usage (/)	2% of 447GiB - ufs

Figura 5. Información General y Estado del Hardware
Tomado de https://192.xxx.x.x:40443

En la figura 5, se visualiza las interfaces configuradas en el firewall, en este caso se tiene 3 interfaces configuradas (WAN, LAN DMZ), donde la interfaz WAN, es la que se encarga de permitir que la interface LAN se conecte a una red amplia, dando acceso a servicio de internet. La interfaz LAN, es donde está configurada la red interna y, permite la conexión directa de clientes hacia servidor firewall.

La interfaz DMZ, está configurada al servidor de correo electrónico, y por la cual se contrala el acceso al mismo mediante equipos externos.

Interfaces

WAN	↑	100baseTX <full-duplex>
LAN	↑	1000baseT <full-duplex>
DMZ	↑	

Interface Statistics

	WAN	LAN	DMZ
Packets In	1704710088	1190149026	141794012
Packets Out	1129746999	1766861570	132867992
Bytes In	1.88 TiB	248.49 GiB	25.84 GiB
Bytes Out	222.10 GiB	1.88 TiB	47.19 GiB
Errors In	0	0	874
Errors Out	0	0	0
Collisions	0	0	669

Figura 6. Interfaces Instaladas y configuradas Firewall JNDA
Tomado de https://192.xxx.x.x:40443

Referente a la figura 7, se puede observar la gráfica de tráfico de datos que cada una de las interfaces está consumiendo, en este caso se identifica que la interfaz con más carga de datos es la WAN, ya que esta abarca las conexiones de las otras interfaces configuradas.

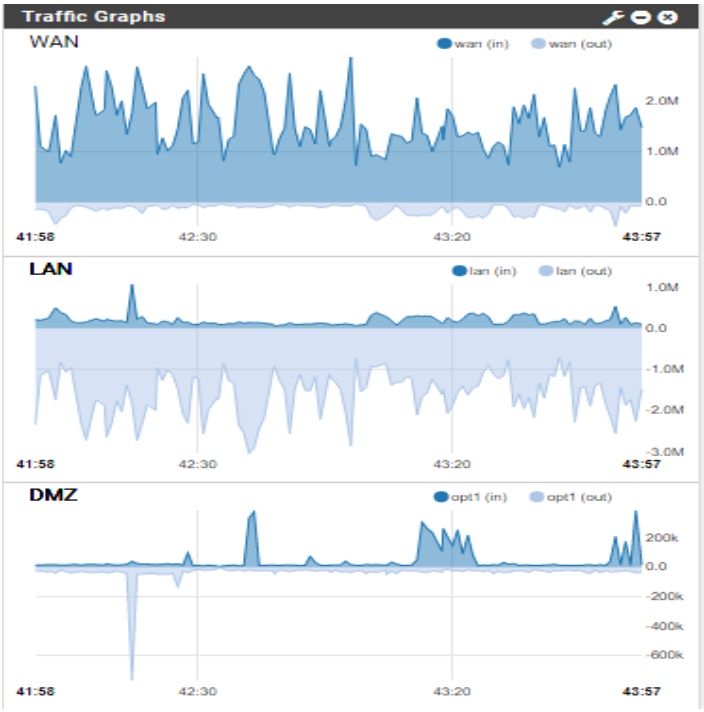


Figura 7. Gráfico Consumo de Tráfico de datos
https://192.xxx.x.x:40443

2.1.2 Antivirus Eset.

ESET Endpoint Security ofrece protección en varias capas para endpoints corporativas gracias a su antivirus, firewall personal, control Web, antispam del cliente y otras características de protección avanzadas y comprobadas para proteger la red esté o no en línea. (ESET, 2017)

2.1.2.1 Administración Eset.

Para la administración de eset, ingresa mediante un computador o dispositivo que esté conectado a la red interna de la JNDA y, utilizando cualquier navegador de confianza; como se observa en la figura 7.

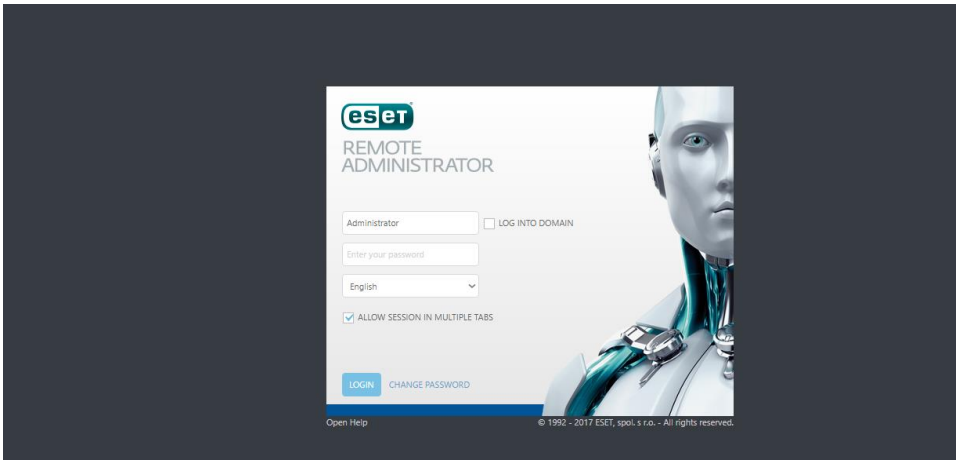


Figura 8. Captura de Pantalla Login Eset JNDA
Tomado de https://antivirus:8443/era/webconsole/

Una vez ingresadas las credenciales, la interface nos redirigirá directamente a la pantalla de dashboard, en donde se podrá visualizar las estadísticas, el estado, la información del sistema, etc.; como se observa en la figura 8.

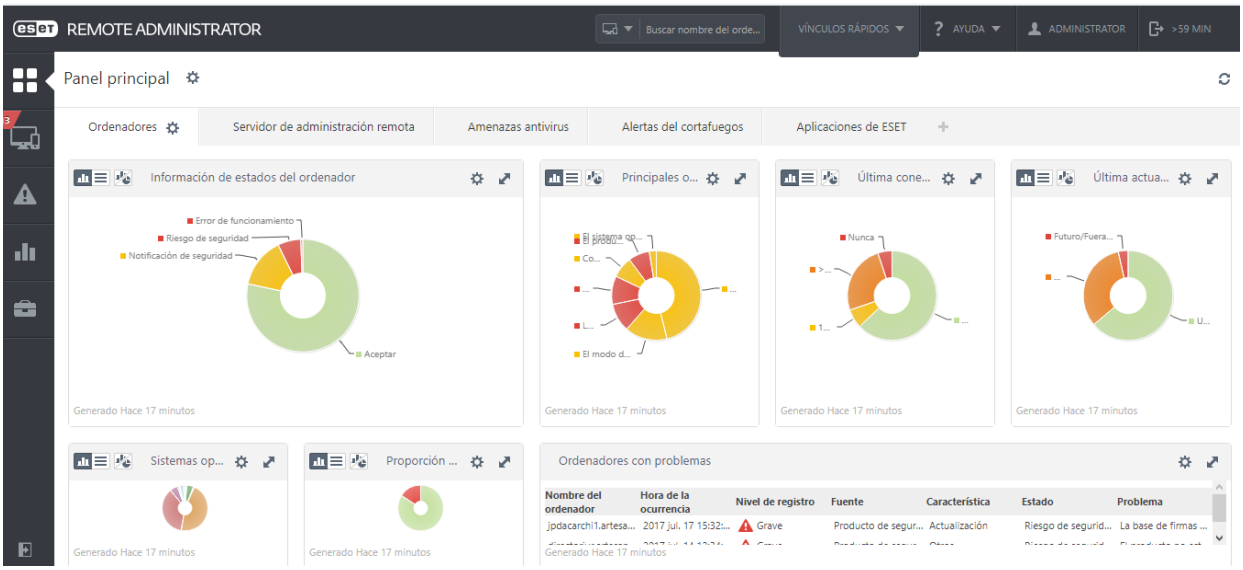


Figura 9. Dashboard ESET JNDA
Tomado de https://antivirus:8443/era/webconsole/#id=DASHBOARDS;u=00000000-0000-0000-7017-000000000001

En la sección de ordenadores con problemas, podemos observar que varios computadores o dispositivos conectados en la red interna de la JNDA, ya sea por su enlace de datos, conexión inalámbrica o red LAN, presentan varias incidencias, como se observa en la figura 8, mismas que serán analizadas en otro punto de este capítulo.

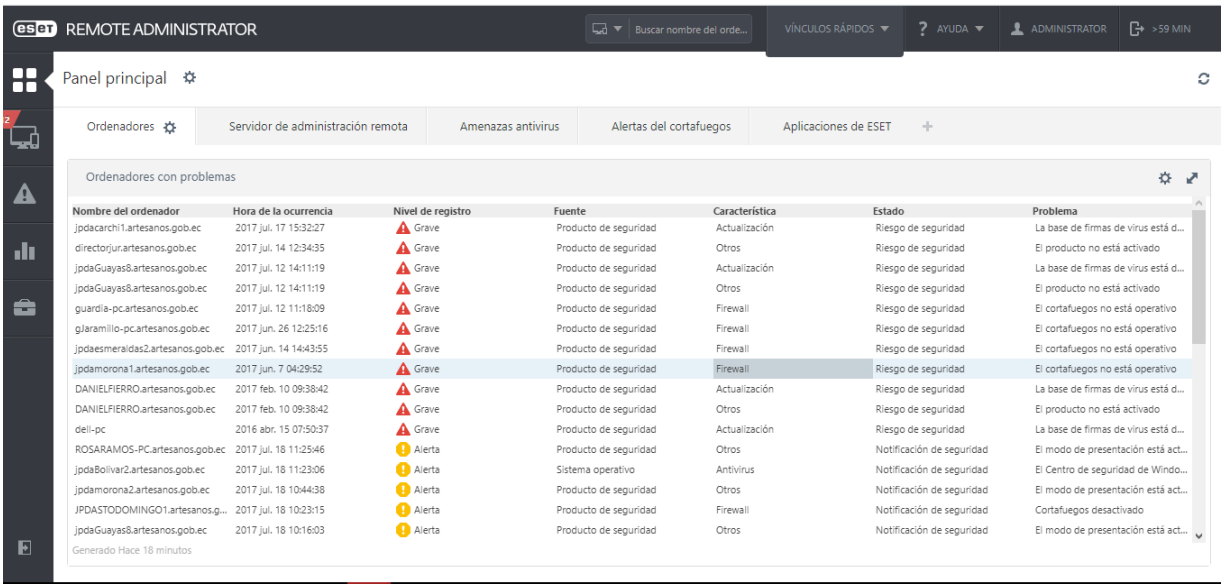


Figura 10. Captura del módulo de problemas
Tomado de https://antivirus:8443/era/webconsole/#id=DASHBOARDS;u=00000000-0000-0000-7017-000000000001

2.2 Estudio de factibilidad para el levantamiento de vulnerabilidades y ataques de red, dentro de la Junta Nacional de Defensa del Artesano.

El presente estudio de factibilidad para el levantamiento de vulnerabilidades se basa en dos aspectos importantes, los cuales son:

- Factibilidad Técnica.
- Factibilidad Operativa.

2.2.1 Factibilidad Técnica.

Dentro de la factibilidad técnica, se concluye que el recurso tecnológico, que actualmente tiene la Junta Nacional de Defensa del Artesano es el siguiente:

Hardware:

Computador:

- Marca: Dell.
- Procesador: Intel® Core™ i7-3540M CPU @ 3.00GHz. 3.00GHz.
- Memoria Ram: 4GB.
- Tipo Sistema: Sistema operativo 64 bits, procesador x64.
- Microsoft Windows 7 o superior (preinstalado).

Servidor:

- Marca: HP.
- Procesador: Intel® Core™ i5-2400 CPU @ 3.10GHz.
- Memoria Ram: 4GB.
- 4 núcleos.
- Controlador de red: 2 Puertos 1 Gabe NC326i.

Software.

Firewall:

- PFSENSE.
- Port: 40443.
- Protocolo: HTTP/HTTPS.
- SSL Certificade: webConfigurator default (575ecd2664bb0).
- SSH port: 2222.

Antivirus:

- Eset Endpoint Security EES.
- ESET Remote Administrator (Server), version 6.5 (6.5.417.0).
- ESET Remote Administrator (Console web), version 6.5 (6.5.388.0).

Periféricos, Interfaces y tecnologías requeridas.

- Interfaz de red ethernet 10/100 Base TX (computador y servidor).
- Tecnología inalámbrica WLAN 802.11b.
- Pantalla Descreen WXGA HD 19 pulgadas (computador y servidor).
- Resolución de pantalla 1600x900 60p Hz. (computador y servidor).
- Tarjeta Gráfica Intel® HD Graphics 4000 (computador y servidor).
- Teclado 82 teclas USB (computador y servidor).

Con este recurso, se concluye que se al momento se cuenta con los equipos suficientes para el alcance del presente trabajo.

2.2.2 Factibilidad Operativa.

Se cuenta con el recurso humano y contingente profesional que labora en la dirección de tecnología de la Junta Nacional de Defensa del Artesano, según el siguiente organigrama operativo:

- Personal que autoriza.
- Personal que supervisa.
- Personal de ejecución.
- Personal de apoyo.

Personal que Autoriza:

Presidente de la Junta Nacional de Defensa Del Artesano.

Personal que Supervisa:

Director de la dirección de tecnología de la Junta Nacional de Defensa del Artesano.

Personal que Ejecuta:

Asistente de la dirección de tecnología de la Junta Nacional de Defensa del Artesano.

Personal de Apoyo:

Analista de la dirección de tecnología de la Junta Nacional de Defensa del Artesano.

2.3 Análisis y auditoría de las posibles vulnerabilidades que tiene la red interna de la Junta Nacional de Defensa del Artesano.

Para el análisis de las posibles vulnerabilidades que tiene la red interna de la Junta Nacional de Defensa del Artesano, se ha utilizado las propias herramientas de seguridad que se encuentran instaladas en la institución, estas son el Firewall y el Antivirus, teniendo como resultando las siguientes vulnerabilidades más comunes.

2.3.1 Problemas a nivel de servidor.

Servidores con Sistema Operativo Windows (aplicativos, software contable y registro artesanal).

Dentro del servidor de aplicativos, servidor de software contable y registro artesanal, se encontraron las siguientes vulnerabilidades:

2.3.1.1 El servidor no tiene habilitado el firewall personal de Windows.

Que el Firewall no este activo, implica que el computador aceptará todo tipo de conexión y tráfico entrante, dejando totalmente vulnerable al equipo para que cualquier atacante o ataque ingrese al ordenador por cualquier puerto de conexión y poniendo a disponibilidad todo tipo de información.

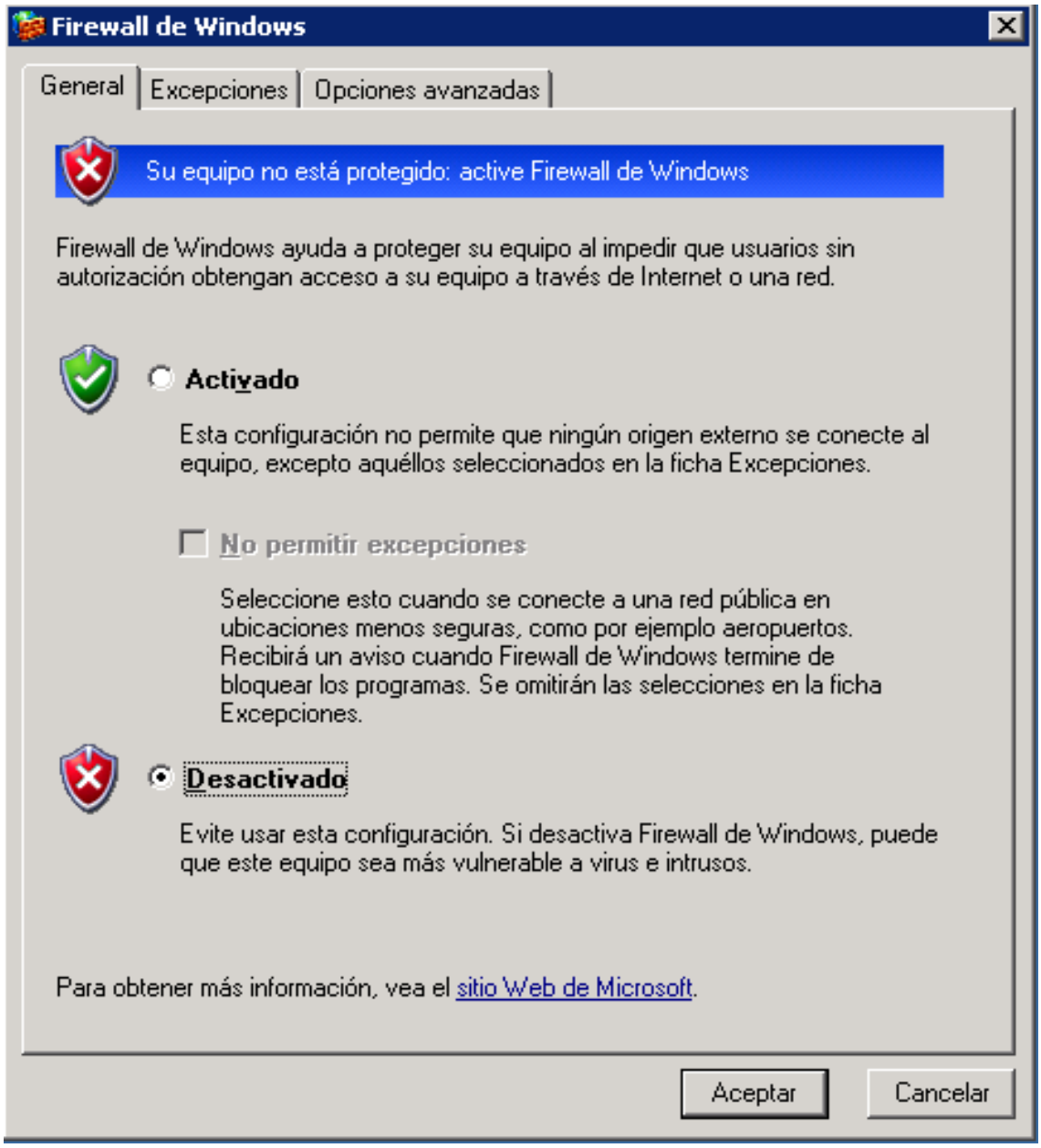


Figura 11. Captura de Pantalla de Configuración de Firewall de Windows, servidor de Aplicativos
Tomado de Servidor de la JNDA

2.3.1.2 El servidor no cuenta con un antivirus instalado.

Al no tener un antivirus instalado localmente en el equipo, implica que el ordenador este propenso a ser víctima de cualquier ataque de virus y a su vez,

el mismo no podrá ser detectado para dar un oportuno procedimiento para su solución.

2.3.2 Problemas a nivel de usuario.

Módulo de Ordenadores con problemas; figura 10.

- La base de protección antiphishing no está operativa.
- La base de firmas de virus está desactualizada.
- El producto no fue activado.
- El cortafuegos no está operativo.
- El centro de seguridad de Windows indica que la función no está instalada. o no funciona correctamente.
- El modo de presentación está activo.

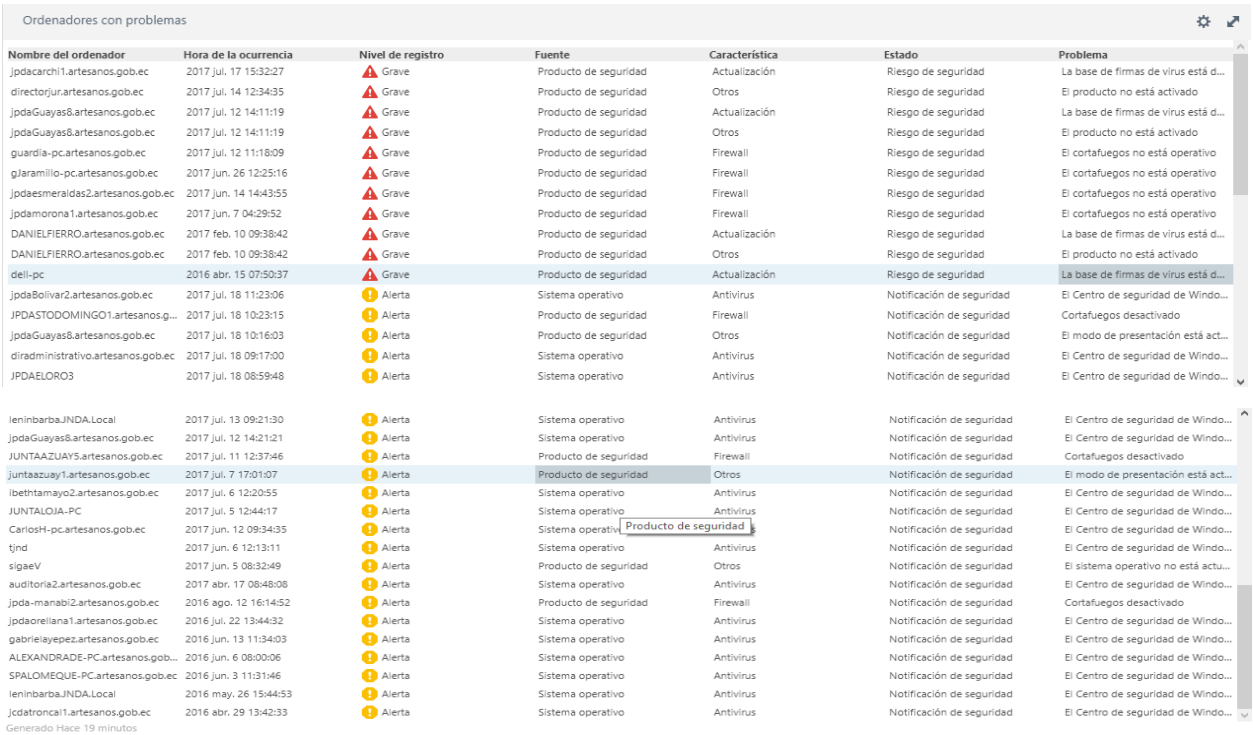


Figura 12. Amenazas Dentro de la red Interna de la JNDA
Tomado de https://antivirus:8443/era/webconsole/#id=DASHBOARDS;u=00000000-0000-0000-7017-000000000001

Con base al análisis realizado al módulo de ordenadores con problemas y, una vez identificados los mismos, se detalla en lo que puede derivar, si no se da la atención o control requerido.

2.3.2.1 La base de protección antiphishing no está operativa.

No tener activa la protección antiphishing, significa que el ordenador no podrá identificar al atacante, de tal manera que el usuario aceptará la información fraudulenta enviada por un medio electrónico (e-mail), suponiendo que la misma es verídica o confiable y, de esta manera el atacante obtendrá datos confidenciales y delicados como: Información detallada de tarjetas de crédito, cuentas bancarias, etc.

2.3.2.2 La base de firmas de virus esta desactualizada.

Al tener desactualizada la base de firmas, implica que el equipo está propenso a ser infectado por algún ataque que no esté identificado dentro del antivirus, o a su vez que el mismo fue actualizado por el atacante, pero el antivirus aún no la ha identificado; de esta manera, el virus o el atacante puede atacar directamente al ordenador, independientemente que el antivirus es operando.

2.3.2.3 El producto no fue activado.

Al no tener el producto activo, implica que la licencia del antivirus no es funcional, o que la misma ya caducó, por lo tanto, el software no tendrá las mismas funcionalidades que cuando estaba activo, lo que puede ser que el equipo este totalmente vulnerable a cualquier ataque, independientemente que el antivirus este instalado.

2.3.2.4 El cortafuego no está operativo.

Que el cortafuego no este activo, implica que el computador aceptará todo tipo de conexión y tráfico entrante, dejando totalmente vulnerable al equipo para que cualquier atacante o ataque ingrese al ordenador por cualquier puerto de conexión y poniendo a disponibilidad todo tipo de información.

2.3.2.5 El centro de seguridad de Windows indica que la función no está instalada o no funciona correctamente.

El centro de seguridad de Windows es aquel que se encarga de comprobar el estado de seguridad del equipo, aspectos como configuración de firewall, entre otros; al no tener esta funcionalidad activa o de por si desinstalada, el sistema operativo no podrá detectar si el equipo está seguro a través de su configuración de seguridad.

2.3.2.6 Módulo de amenazas.

En el módulo de amenazas se determina cuáles son los principales usuarios con vulnerabilidad de amenaza en los últimos siete días; como se observa en la figura 11.

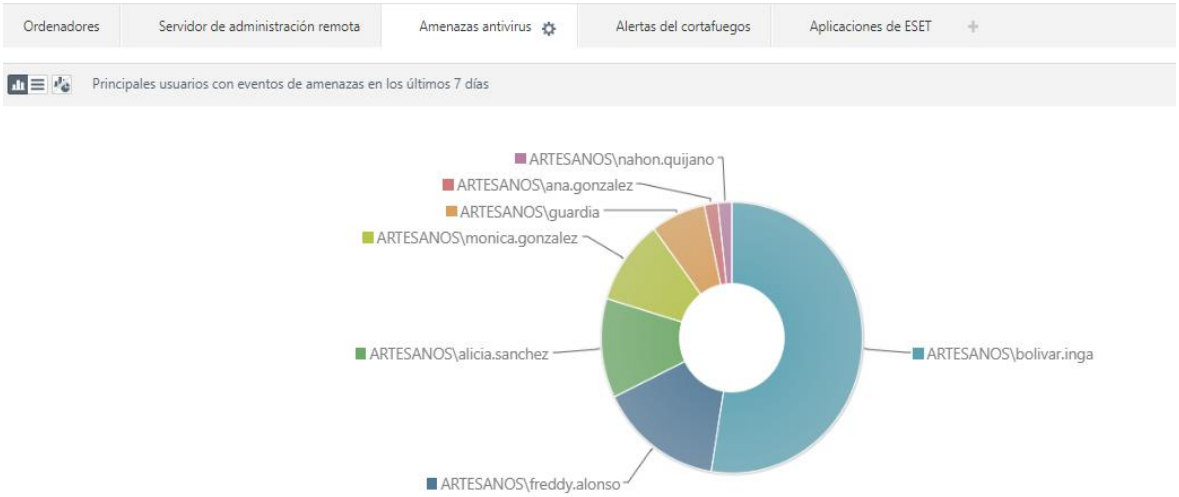


Figura 13. Gráfica Estadística de Usuarios/Equipos con más Incidencia Tomado de Amenazas https://xxx.xxx.xx.5:40443/diag_arp.php

Se puede observar las amenazas, ataques e incidencias más comunes y analizadas y/o auditadas en la red interna de la Junta Nacional de Defensa del Artesano; Tabla 3.

Tabla 3.
Amenazas e Incidencias más Comunes en la red Interna de la JNDA

TIPO DE AMENAZA O ATAQUE	**NOMBRE DE LA AMENAZA O ATAQUE**	**BASE DE FIRMAS DE VIRUS**
Gusano	Win32/Autoit.OB	15760 20170717)
Gusano	Win32/Autoit.OB	15772 (20170719)
Troyano	LNK/Agent.CX	15760 (20170717)
Troyano	LNK/Agent.CX	15772 (20170719)
Troyano	LNK/Agent.DX	15760 (20170717)
Gusano	Win32/Autoit.OB	15772 (20170719)
Troyano	LNK/Agent.CY	15748 (20170714)
Aplicación/Adwarwe	S/Adware.BNXAds.A	15755 (20170716)
Aplicación/Adware	JS/Adware.BNXAds.A	15755 (20170716)

2.3.2.7 Gusano Win32/Autoit.OB.

Es un virus tipo “gusano”, cuya creación fue detectada el 3 de julio de 2017 y su versión de base de datos es la 15685, prevalece principalmente en las zonas de américa del sur, puntualmente en Perú y Bolivia. (Eset, 2017)

2.3.2.8 Troyano LNK/Agent.CX.

Es un virus tipo “troyano”, cuya creación fue detectada el 31 de mayo de 2016 y su versión de base de datos es la 13573, prevalece principalmente en las zonas de américa del sur, puntualmente en Perú, Ecuador y Bolivia; ataque principalmente a los equipos con sistema operativo Windows y su objetivo es pretender que el usuario crea en una serie de programas positivos, para que una vez instalados, estos ataquen al equipo con programas maliciosos. (Eset, 2017)

2.3.2.9 Adware S/Adware.BNXAds.A.

Es un virus de tipo “adware”, cuya creación fue detectada el 9 de mayo del 2017 y su versión de base de datos es la 15388, prevalece principalmente en las zonas de Europa, Asia y África, puntualmente en Ucrania, Tailandia y Rusia, se encarga de la entrega de anuncios no deseados o solicitados por protocolo HTTP. (Eset, 2017)

CAPITULO III: Elaboración de la propuesta de medidas de mitigación contra las vulnerabilidades y ataques informáticos más comunes dentro de la red interna de la Junta Nacional de Defensa del Artesano.

En el presente proyecto, para la elaboración de la propuesta de medidas de mitigación contra las vulnerabilidades y ataques informáticos más comunes dentro de la red interna de la Junta Nacional de Defensa del Artesano, únicamente se utilizará el recurso tecnológico disponible en la institución y a su vez, mecanismos que no requieran de incursión de presupuesto para su ejecución o adquisición de equipos adicionales o contratación de personal.

3.1 Elaboración de la propuesta de medidas de mitigación contra los ataques informáticos más comunes dentro de la red interna de la Junta Nacional de Defensa del Artesano.

Una vez analizados y auditados los posibles ataques, vulnerabilidades y amenazas más comunes que presenta la red interna de la Junta Nacional de Defensa del Artesano, se procede a presentar la propuesta de medidas de mitigación, el mismo que contiene el plan de seguridad informática institucional; esto en relación con lo mencionado inicialmente.

3.1.1 Soluciones a ataques y vulnerabilidades a nivel de servidor.

Para los ataques y vulnerabilidades encontradas en la red interna de servidores de la JNDA, se dispone las siguientes posibles soluciones para mitigar las mismas.

3.1.1.1 Solución para la vulnerabilidad de que servidor no tiene habilitado el firewall personal de Windows.

Se dispone habilitar el firewall personal de Windows, sin dejar que este pierda conexión con los otros equipos y el acceso a internet, esto se lo puede realizar configurando reglas dentro del firewall, habilitando puertos seguros y de confianza y deshabilitando los que no tengan relación con las actividades habituales de trabajo en el servidor.

3.1.1.2 Solución para la vulnerabilidad que el servidor no cuenta con un antivirus instalado.

Se dispone la instalación del antivirus adquirido ya por la institución, en este caso el Eset Endpoint Security (EES), pero en su versión para servidores; ya que, por tratarse de un servidor, este es propenso a sufrir cualquier tipo de ataques o caída de servicio y no maneja la misma configuración de seguridad que luna máquina de usuario común.

3.1.2 Soluciones para ataques y vulnerabilidades a nivel de usuario.

Para los ataques y vulnerabilidades encontradas en la red interna de la JNDA, se dispone implantar las siguientes soluciones para mitigar las mismas.

3.1.2.1 Solución ante la vulnerabilidad de “la base de protección antiphishing no está operativa”.

Ante dicha vulnerabilidad, lo primordial es saber identificar el destino o proveniencia del correo, publicidad o medio electrónico por el cual el atacante se han puesto en contacto con el usuario, ya que las instituciones, en este caso financieras, generalmente nunca solicitan información relacionada con claves de tarjeta de crédito o débito, tampoco números completos de cuentas bancarias,

por lo tanto, este es el procedimiento sugerido para no ser víctima de esta vulnerabilidad:

- Aprender a identificar claramente los correos aparentemente sospechosos, en el caso de serlo o tener duda sobre uno de ellos, comunicar de inmediato al administrador de red.
- Verificar la fuente de la cual fue enviado la solicitud o notificación, esto se lo puede hacer confirmando el dominio al cual pertenece el correo enviado, de tener dudas, contactar a la institución para corroborar directamente con ellos si dicha información es verídica.
- Por ningún motivo, entrar a la web de la institución financiera mediante links enviados por correo electrónico, ya que esta puede redirigir a una web similar de la misma, siendo a la final la página del atacante.
- Crear una regla en el antivirus, la cual bloquee este tipo de ataques.
- Al momento de introducir información personal dentro de cualquier formulario en la web, hacerlo siempre de una que sea segura, esto se lo puede hacer comprobando que antes del URL en la barra de dirección comience con “https://”, seguido de la dirección de la página.
- Tener control periódico de las cuentas bancarias, esto con el fin de comprobar si ha habido algún tipo de irregularidad y poder notificarla a tiempo.
- Tener en cuenta la configuración habitual que tiene para el ingreso de credenciales, si se identifica algo diferente, como por ejemplo el idioma, desistir del ingreso de datos.
- No abrir correos electrónicos ni adjuntos a los mismos, que no tengan relación a su actividad diaria.
- No proporcionar información confidencial o privada por teléfono o correo electrónico.
- Mantener el sistema operativo y el navegador habitual actualizado, ya que de esta manera el riesgo de sufrir uno de estos ataques disminuye, ya que la seguridad por defecto que estos traen también estará actualizada.

- Reforzar a los usuarios con charlas de seguridad referente a este tipo de ataques, así la prevención será mayor por parte del administrador y el usuario final.

A pesar de este plan de seguridad, resulta casi imposible frenar todos los ataques “phishing”, por lo que tener una cultura prudente y de prevención ante los mismos resultará en una gran disminución de probabilidad de poder ser víctima de este tipo de ataques.

3.1.2.2 Solución ante la vulnerabilidad “la base de firmas de virus está desactualizada”.

En relación con esta vulnerabilidad, se deber tener en cuenta que, independientemente la operatividad que el antivirus tenga en el equipo, este no podrá prevenir ni corregir virus que han sido actualizados, que solo tendrá en su sistema de protección, ataques ya identificados, es decir, base de firmas de virus reconocidos anteriormente, por lo tanto, este es el procedimiento a seguir para evitar este tipo de vulnerabilidades:

- Actualizar manualmente el antivirus instalado.
- Programar una tarea dentro del el servidor que administra el antivirus, para que todos los clientes actualicen su base de firmas al mismo tiempo, de esta manera se mantendrá el control colectivo de todos los equipos.
- Identificar cuáles son los equipos que no han recibido la actualización, determinar el motivo y de ser posible reinstalar el software de antivirus.

3.1.2.3 Solución ante la vulnerabilidad “el producto no fue activado”.

En relación con dicha vulnerabilidad, se debe tomar en cuenta que independientemente que el antivirus este instalado, este no es totalmente

funcional, ya que, en versiones licenciadas, se obtiene servicios adicionales, para lo cual, el siguiente procedimiento, ayudará a solventar dicho problema:

- Adquirir un antivirus con el número de licencias requeridas, estas licencias pueden tener la durabilidad que el administrador requiera según sus necesidades.
- Si el producto ya caducó o está por caducar, proceder con la solicitud anticipada y oportuna de renovación de licencia, esto con el fin de no perder el servicio de protección licenciado en ningún momento.
- De no estar satisfecho con el servicio de protección brindado por el antivirus, informarse de otras soluciones similares, mismas que se acomoden al presupuesto y a las necesidades institucionales.
- Considerar la posibilidad de que distribuidores autorizados en las diferentes marcas, ofrezcan una solución de prueba, esto con el fin de que el administrador lo evalúe.
- Verificar que no esté instalado más de un antivirus, ya que esto puede generar conflicto entre ellos.

3.1.2.4 Solución ante la vulnerabilidad “el cortafuego no está operativo”.

En referencia al error presentado, se debe tomar en cuenta que, este error está relacionado al firewall de Windows, es decir al firewall del sistema operativo, ya que en la JNDA también se trabaja con un firewall de frontera; para solventar dicho problema, se dispone seguir las siguientes indicaciones:

- Configurar las reglas de conexiones entrantes y salientes dentro del firewall de frontera(PFSENSE), esto con el fin de permitir únicamente el tráfico de datos y servicios de confianza.

- Configurar los puertos de conexión de confianza, por ejemplo, para el envío y recepción de correos, se necesitará habilitar los puertos 110(POP3) y 25(SMTP), de ser el caso.
- Configurar reglas de firewall para acceso a diferentes páginas web, según perfiles de usuario, esto con el fin de optimizar los recursos de ancho de banda.

En algunos casos, al habilitar el firewall de Windows, las conexiones tales como las de internet, podrían presentar problemas como bloquear el servicio, por tanto, si se tiene dicho inconveniente, se deberá deshabilitar el firewall de Windows, para que el firewall del antivirus o el de frontera, sea el rector de las conexiones.

3.1.2.5 Solución ante la vulnerabilidad “el centro de seguridad de Windows indica que la función no está instalada o no funciona correctamente”.

Si bien dicho, este mensaje no refiere directamente a un ataque, pero el mismo es el encargado de comprobar el estado y configuración del equipo, para lo cual se debe seguir el siguiente procedimiento para su optimización:

- Instalar o habilitar la herramienta de centro de seguridad de Windows, ya que la misma orientará e informará al administrador el estado de seguridad básico del equipo, como también su configuración actual.

3.1.2.6 Métodos de protección y prevención contra ataques encontrados en el módulo de amenazas de la red de la Junta Nacional de Defensa del Artesano.

Tomando en cuenta los ataques encontrados, se debe considerar el siguiente procedimiento, como solución, para que en un futuro estas puedan ser prevenidas:

- Tener instalado un sistema de antivirus, mismo que tiene que estar activo, actualizado y licenciado.
- Ejecutar tareas periódicas de detección de virus, esto con el fin de tener una red totalmente protegida.
- Identificar las máquinas con mayor número de incidencias, esto con el fin de aislar al equipo para evitar el contagio a otros computadores.
- Verificar la causa de infección al equipo, con el propósito de poder corregir el inconveniente y prevenir un nuevo ataque.
- Analizar los archivos infectados, para identificar cual fue su procedencia.
- Mover a cuarentena los archivos que no pueden ser desinfectados.
- Restringir el acceso de dispositivos de almacenamiento masivo ajenos a la institución, de ser necesario su uso, notificar dicha solicitud al administrador de la red.
- Restringir el acceso de dispositivos de almacenamiento óptico ajenos a la institución, de ser necesario su uso, notificar dicha solicitud al administrador de la red.
- Configurar un sistema de anti spam, con el fin de poder enviar y recibir correos legítimos, evitando caer en listas negras.

3.2 Medidas de protección y mitigación contra posibles ataques informáticos, que podrían vulnerar la seguridad de la red interna de la Junta Nacional de Defensa del Artesano.

La JNDA, por ser un ente de derecho público, maneja información pública, misma que puede ser de interés para los atacantes debido al contenido de esa información, por lo dicho, los ataques que podría afectar a la red interna son los siguientes:

- DoS
- DDoS
- Ingeniería Social

3.2.1 Protección contra los ataques de DoS.

Es necesario revisar la configuración de Routers y Firewalls para detener IPs inválidas, así como también el filtrado de protocolos que no sean necesarios. Algunos firewalls, tienen la opción de prevenir inundaciones (floods) en los protocolos TCP/UDP. Además, es aconsejable habilitar la opción de logging (logs) para llevar un control adecuado de las conexiones que existen con dichos routers.

Otras de las opciones que se deben tener en cuenta es solicitar ayuda al Proveedor de Servicios de Internet (ISP). Con esto, se puede bloquear el tráfico más cercano a su origen sin necesidad de que alcance a la organización. (Catoira, 28).

Según (Catoira, 28), algunos consejos técnicos para evitar ataques DoS son:

- Limitar la tasa de tráfico proveniente de un único host.
- Limitar el número de conexiones que lleguen al servidor.
- Limitar el uso del ancho de banda por aquellos hosts que cometan abusos de red.
- Ejecutar un monitoreo de las conexiones que se llevan a cabo en el servidor (permite identificar patrones de ataque).

3.2.2 Protección contra los ataques de DDoS.

Según (Salom, 2014), la manera más óptima de prevenir ataques DDoS, es con el siguiente procedimiento:

- El primer paso para lograr protección contra ataques DDoS consiste en mantener todos los equipos con antivirus actualizados y monitorizar la actividad anómala dentro de nuestra red.
- El segundo paso, consiste en dimensionar de forma adecuada nuestros sistemas. A menudo se confunden volúmenes de tráfico lícitos con ataques de denegación. Incluso los tráficos generados por las herramientas de indexación de Google pueden “tumbar” una web que no esté preparada para gestionarlo adecuadamente. En este sentido es importante contar con infraestructuras flexibles, que puedan proporcionar capacidad on-demand y que puedan soportar necesidades de negocio crecientes.
- El tercer y último paso para conseguir protección contra ataques DDoS, consiste en tener equipos propios de seguridad especializados, mismos que se interpongan entre el atacante y la infraestructura de red.

3.2.3 Protección contra ataques de ingeniería social.

Para (Navarro, 2011), los métodos más comunes para evitar ataques de ingeniería social son:

- En ningún momento se debe mencionar por teléfono o confidenciales como claves de acceso, números de tarjetas de crédito, cuentas bancarias, etc.
- Jamás hacer click en un enlace a una página web que le llegue a través de un e-mail en el que le piden datos personales.
- Desconfiar de cualquier tipo correo electrónico en el que se le ofrece la posibilidad de ganar dinero fácil.
- Si es usuario de banca electrónica o de cualquier otro servicio que implique introducir datos en una web, afirmar que la dirección de la web es correcta.

- No confíe en las direcciones de los intermediarios de correo o en los identificadores del número llamante en el teléfono: pueden falsearse con suma facilidad.
- Instale en su ordenador un buen software de seguridad que incluya si es posible funcionalidad antivirus, antiphising, antispyware y antimalware para minimizar los riesgos.
- Utilice el sentido común y pregúntese siempre que reciba un mensaje o llamada sospechosa si alguien puede obtener algún beneficio de forma ilícita con la información que le solicitan.

CAPITULO IV: Conclusiones y Recomendaciones

4.1 Conclusiones y Recomendaciones.

4.1.1 Conclusiones

- A lo largo de la presente investigación, se logró demostrar que la red informática interna de la Junta Nacional de Defensa del Artesano cuenta con algunas herramientas de seguridad, pero estas a su vez, no están siendo utilizadas al máximo de su capacidad, ya que se pudo observar que presentan varios ataques y vulnerabilidades que pueden afectar el desempeño de los ordenadores.

- Con lo expuesto anteriormente, se puede concluir que si no se da atención oportuna y pertinente a los ataques y vulnerabilidades encontradas, estas pueden generar diversos inconvenientes al usuario y más al administrador de la red, tomando en cuenta que la mayoría de ellas son manejables y se las pueden evitar; a su vez, se pudo determinar que la información que maneja la Junta Nacional de Defensa del Artesano, es bastante delicada, ya que se trata de datos personales relacionados con el artesano y su taller, misma que podría ser de gran interés para un posible atacante, de tal manera que puede ser mal utilizada, al punto de que podría ser eliminada totalmente, generando inconvenientes entre la institución y el artesano.

- La JNDA, cuenta con un nivel básico de seguridad, mismo que podría estar expuesto a ataques informáticos, derivando en pérdidas y filtración de información sensible, pérdida de recursos de red, bloqueos y negación de servicios, pérdida del control total de infraestructura de red, etc.

- La JNDA, no cuenta con un plan de mitigación interno, contra ataques, amenazas y vulnerabilidades que puedan presentarse.

4.1.2 Recomendaciones

- Si bien este trabajo de investigación no representa un solución total a todos los ataques y vulnerabilidades que tiene la red interna de la Junta Nacional de Defensa del Artesano, sino a los más comunes, se recomienda implementar esta propuesta de mitigación como posible solución a las incidencias encontradas, esto con el fin de prevenir futuros ataques y amenazas, que pongan en riesgo el desarrollo normal de las actividades institucionales y, además, corregir los problemas ya detectados e identificados.

- Elaborar un manual de procedimientos de seguridad, en el cual conste el proceso a realizar en caso de detectarse o de sospechar la presencia de una posible vulnerabilidad, esto con el fin de que el usuario pueda reaccionar de manera oportuna ante estas eventualidades.

- Generar un ambiente de confianza entre el administrador de la red y el usuario común, ya que, mediante capacitaciones y charlas de seguridad por parte del administrador, el usuario puede familiarizarse más con el computador, entendiendo cuales son los riesgos que puede correr si no se sigue el manual de procesos recomendado.

- Socializar entre los administradores de red y los usuarios, las ventajas de tener un sistema seguro, eso en beneficio de la institución, de tal manera que se convierta en un trabajo mancomunado, que no necesariamente tiene que ser tedioso y, por último, tratar de quitar el miedo que tiene el usuario con el computador, explicando que es medio de trabajo esencial para el desarrollo y profesional de cada individuo.

- Incluir dentro del Plan Anual de Compras (PAC) 2018, la adquisición de una solución de anti spam, para proteger el sistema de correo electrónico.
- Designar un profesional afín a la seguridad informática, para que este sea el encargado de asumir todas las competencias relacionadas con la seguridad de la rede de la JNDA.

- Programar tareas periódicas de revisión de virus a los equipos de usuarios y servidores, eso sin afectar el normal desempeño de la red ni interrumpir las tareas diarias de los funcionarios.

- Generar políticas de acceso por perfiles, en las cuales sea necesario el ingreso de usuario y contraseña para cualquier proceso de ejecución o instalación de programas.

- Programar un respaldo automático de información a un servidor que esté protegido, esto con el fin de que, en el caso de sufrir algún tipo de ataque, esta información este respaldada para su inmediato uso.

- Bloquear el acceso a páginas ajenas al trabajo que cada funcionario tiene asignado.

- Bloquear el acceso a puertos de conexión ajenos a las actividades institucionales.

REFERENCIAS

Álvarez Marañón, G., & Pérez García, P. P. (2004). *SEGURIDAD INFORMÁTICA PARA EMPRESAS Y PARTICULARES.* MADRID: Mc Graw Hill.

Bembibre, V. (30 de 12 de 2008). *Definición ABC*. Obtenido de https://www.definicionabc.com/tecnologia/antivirus.ph

CATOIRA, F. (20 de 12 de 2013). *welivesecurity*.

Catoira, F. (2012 de 03 de 28). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/

Dordoigne, J. (2015). *Redes Informáticas Nociones Fundamentales (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP V6).*

Eset. (19 de 07 de 2017). Obtenido de Virus Radar: http://www.virusradar.com/en/Win32_Autoit.OB/description

Eset. (19 de 07 de 2017). Obtenido de Virus Radar: http://www.virusradar.com/en/LNK_Agent.CX/description

Eset. (07 de 19 de 2017). Obtenido de Virus Radar: http://www.virusradar.com/en/JS_Adware.BNXAds/map

ESET. (18 de 07 de 2017). Obtenido de https://tienda.eset.com.ec/?gclid=CjwKCAjw47bLBRBkEiwABh-PkestKeDWOCIseNw2fG1ol9-kSzM-dmPQ8qEWXfzjowFCPpDExa4MrBoCG5YQAvD_BwE#/empresas#pack_seguridad

Estrada, A. C. (2016). *Seguridad en Redes.* Madrid.

Larrieu, C. (29 de 01 de 2003). *CCM*. Obtenido de http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

Navarro, A. N. (31 de 01 de 2011). *TICS Consulting - Consultoría y seguridad*. Obtenido de http://www.ticsconsulting.es/blog/generar-claves-seguras-3

PFSENSE. (17 de 07 de 2017). Obtenido de https://www.pfsense.org/getting-started/

Roa Buendía, J. F. (2013). *Seguridad informática.* McGraw-Hill Interamericana.

Salom, J. (20 de 08 de 2014). *Claranet Spain*. Obtenido de https://www.claranet.es/blog/proteccion-contra-ataques-dos-ddos-proveedor-servicio.html

Stallings, W. (2004). *FUNDAMENTOS DE SEGURIDAD EN REDES* (Vol. Segunda Edición). Madrid: PEARSON EDUCACIÓN S.A.

Tanenbaum, A. S. (2012). *Redes de Computadoras* (Vol. IIII). (G. Trujano Mendoza, Ed.) Ciudad de Mexico, Mexico: Pearson Prentice Hall.

ANEXOS

ANEXO 1.

Amenazas Activas detectadas por el antivirus interno de la JNDA.

ESET REMOTE ADMINISTRATOR

GENERADO EN 2017 jul. 18 14:52:23 (UTC-05:00)

Nombre del ordenador	Tipo de amenaza	Nombre de la amenaza	Indicadores de amenazas	Analizador	Base de firmas de virus	Tipo de objeto	URL del objeto	Acción realizada	Error de la acción	Amenaza gestionada	Se necesita reiniciar el ordenador	Usuario	Nombre del proceso	Circunstan	Hora de la ocurrencia
yeseniave.artesanos.gob.ec	aplicación potencialmente no segura	Win32/HackTool.WinActivator.N		Análisis a petición	14199 (20160929)	archivo	file:///C:/Users/alex.andrade/AppData/Local/Google/Chrome/User Data/Default/File System/001/t/00/00000000/CW.exe		la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator			2016 sept. 29 13:19:59
yeseniave.artesanos.gob.ec	aplicación potencialmente no segura	Win32/HackTool.WinActivator.N		Análisis a petición	14199 (20160929)	archivo	file:///C:/Documents and Settings/alex.andrade/Configuración local/Google/Chrome/User Data/Default/File System/001/t/00/00000000/CW.exe		la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator			2016 sept. 29 13:06:34
yeseniave.artesanos.gob.ec	aplicación potencialmente no segura	Win32/HackTool.WinActivator.N		Análisis a petición	14199 (20160929)	archivo	file:///C:/Documents and Settings/alex.andrade.ARTESANOS/Downloads/CHEW-WGA-BY_CHRIZ.rar/CW.exe		la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator			2016 sept. 29 13:07:59
yeseniave.artesanos.gob.ec	aplicación potencialmente no segura	Win32/HackTool.WinActivator.N		Análisis a petición	14199 (20160929)	archivo	file:///C:/Users/alex.andrade/Configuración local/Google/Chrome/User Data/Default/File System/001/t/00/00000000/CW.exe		la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator			2016 sept. 29 13:21:13
yeseniave.artesanos.gob.ec	aplicación potencialmente no segura	Win32/HackTool.WinActivator.N		Análisis a petición	14199 (20160929)	archivo	file:///C:/Users/alex.andrade.ARTESANOS/Downloads/CHEW-WGA-BY_CHRIZ.rar/CW.exe		la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator			2016 sept. 29 13:22:34
yeseniave.artesanos.gob.ec	aplicación potencialmente no segura	Win32/HackTool.WinActivator.N		Análisis a petición	14199 (20160929)	archivo	file:///C:/Documents and Settings/alex.andrade/AppData/Local/Google/Chrome/User Data/Default/File System/001/t/00/00000000/CW.exe		la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator			2016 sept. 29 13:05:15

jpdaselena1.artesanos.gob.ec	aplicación potencialmente no segura	MSIL/HackTool.WinActivatorA	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/Documents and Settings/USUARIO/Configuración local/Temp/RarSFX0/oem.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no			2016 mar. 4 12:29:56
jpdaselena1.artesanos.gob.ec	aplicación potencialmente no segura	MSIL/HackKMS.G	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/Documents and Settings/Administrador.USUARIO-PC/Desktop/Microsoft Toolkit.exe/deobfuscated.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no			2016 mar. 4 12:06:31
jpdaselena1.artesanos.gob.ec	aplicación potencialmente no segura	MSIL/HackKMS.G	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/Users/Administrador.USUARIO-PC/Desktop/Microsoft Toolkit.exe/deobfuscated.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no			2016 mar. 4 12:34:15
jpdapasta za2.artesanos.gob.ec	aplicación potencialmente no deseada	Win32/YourFileDownloaderA	Variante	Análisis a petición	13682 (20160621)	archivo	file:///E:/documentos de eva del ceta y libro N2/curso de cosmetologia/Cosmetologia_pdf_downloader_2.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ARTESANOS\eva.zuñiga		2016 jun. 21 09:54:58
JPDAORELLANA1.artesanos.gob.ec	troyano	Win32/HoudRat.A	Variante	Protección del sistema de archivos en tiempo real	14311 (20161020)	archivo	file:///G:/AntiUsbShortCut/AntiUsbWorm.zip/script.bin		no	no	ARTESANOS\bolivaringa	C:\Windows\explorer.exe	Se produjo un suceso mientras se intentaba acceder al archivo. 2016 oct. 2011:03:01
JPDAORELLANA1.artesanos.gob.ec	troyano	Win32/HoudRat.A	Variante	Protección del sistema de archivos en tiempo real	14311 (20161020)	archivo	file:///G:/AntiUsbShortCut/AntiUsbShortCut.zip/script.bin		no	no	ARTESANOS\bolivaringa	C:\Windows\explorer.exe	Se produjo un suceso mientras se intentaba acceder al archivo. 2016 oct. 2011:02:59
JPDAORELLANA1.artesanos.gob.ec	aplicación potencialmente no segura	Win32/HiddenStart.A	Variante	Análisis a petición	13846 (20160722)	archivo	file:///C:/Windows/Setup/Scripts/win7T.exe/AutoPlay/Docs/hstart.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ARTESANOS\bolivaringa		2016 jul. 22 15:28:45
JPDAORELLANA1.artesanos.gob.ec	aplicación potencialmente no segura	MSIL/RunElevated.A	Variante	Análisis a petición	13846 (20160722)	archivo	file:///C:/Program Files (x86)/MyPC Backup/Configuration Updater.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ARTESANOS\bolivaringa		2016 jul. 22 15:20:47
jpdaorellana1.artesanos.gob.ec	gusano	Win32/Bundpil.CS	Variante	Análisis en el inicio	13293 (20160406)	archivo	file:///C:/Users/junta/AppData/Local/Temp/cdo1966055469.dll	no se puede desinfectar	no	no			2016 abr. 6 09:28:01
jpdaorellana1.artesanos.gob.ec	gusano	Win32/Bundpil.CS	Variante	Análisis en el inicio	12634 (20151127)	archivo	file:///C:/Users/junta/AppData/Local/Temp/cdo2771071482.dll	no se puede desinfectar	no	no	JPDAORELLANA1\junta		2016 abr. 4 19:32:06

ESET REMOTE ADMINISTRATOR

jpdaorellana1.artesanos.gob.ec	gusano	Win32/Bundpil.CS	Variante	Análisis en el inicio	13287 (20160405)	archivo	file:///C:/Users/junta/AppData/Local/Temp/cdo346714734 7.dll	no se puede desinfectar	no	no		2016 abr. 5 12:53:26
jpdaorellana1.artesanos.gob.ec	aplicación potencialmente no segura	Win32/HiddenStart.A	Variante	Análisis a petición	13298 (20160407)	archivo	file:///C:/Windows/Setup/Scripts/win7T.exe/AutoPlay/Docs/hstart.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	JPDAORELLANA1\junta	2016 abr. 7 09:46:35
jpdaorellana1.artesanos.gob.ec	aplicación potencialmente no segura	MSIL/RunElevated.A	Variante	Análisis a petición	13298 (20160407)	archivo	file:///C:/Program Files (x86)/MyPCBackup/Configuration Updater.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	JPDAORELLANA1\junta	2016 abr. 7 09:14:44
jpdanapo1.artesanos.gob.ec	troyano	Win32/KryptikAESY	Variante	Análisis en el inicio	14531 (20161130)	archivo	file:///C:/Windows/System32/notepad.exe	error al realizar la acción	no	no		2016 nov. 30 15:36:47
jpdamoro na3	aplicación potencialmente no deseada	Win32/TooIbarSoftomate.A	Variante	Análisis a petición	13916 (20160805)	archivo	file:///C:/System Volume Information/_restore{1EBCD62A-D188-4755-A4D9-C81365DB059A}/RP506/A0113806.dll	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no		2016 ago. 5 12:05:00
jpdamoro na3	aplicación potencialmente no deseada	Win32/TooIbarSoftomate.A	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/Documents and Settings/Administrador/Mis documentos/Descargas/chatvibes105.exe/chatvibes.cab/tbcore3.dll	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator	2016 mar. 4 12:19:25
jpdamoro na3	aplicación potencialmente no deseada	Win32/TooIbarSoftomate.A	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/Documents and Settings/Administrador/Datos de programa/Mozilla/Firefox/Profiles/vtyyg0gq.default/extensions/{C9B68337-E93A-44EA-94DC-CB300EC06444}/chrome/content/id_imboost4web_v6/tbcore3.dll	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator	2016 mar. 4 12:18:36
jpdamoro na3	aplicación potencialmente no deseada	Win32/TooIbarSoftomate.A	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/System Volume Information/_restore{1EBCD62A-D188-4755-A4D9-C81365DB059A}/RP488/A0110407.dll	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator	2016 mar. 4 12:24:28

jpdamoro na3	aplicación potencialmente no deseada	Win32/Toolbar.Iminent.E	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/System Volume Information/_restore{1EBCD62A-D1BB-4755-A4D9-C81365DB059A}/RP485/A0109932.rbf	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator	2016 mar. 4 12:23:53
jpdamoro na3	aplicación potencialmente no deseada	Win32/Toolbar.Iminent.E	Variante	Análisis a petición	13916 (20160805)	archivo	file:///C:/System Volume Information/_restore{1EBCD62A-D1BB-4755-A4D9-C81365DB059A}/RP506/A0113802.exe	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no		2016 ago. 5 12:05:00
jpdamoro na3	aplicación potencialmente no deseada	Win32/Toolbar.Iminent.E	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/System Volume Information/_restore{1EBCD62A-D1BB-4755-A4D9-C81365DB059A}/RP485/A0109954.rbf	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator	2016 mar. 4 12:23:54
jpdamoro na3	aplicación potencialmente no deseada	Win32/Toolbar.Iminent.E	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/System Volume Information/_restore{1EBCD62A-D1BB-4755-A4D9-C81365DB059A}/RP485/A0109965.rbf	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator	2016 mar. 4 12:23:55
jpdamoro na3	aplicación potencialmente no deseada	Win32/Toolbar.Iminent.E	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/System Volume Information/_restore{1EBCD62A-D1BB-4755-A4D9-C81365DB059A}/RP485/A0109982.rbf	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator	2016 mar. 4 12:23:56
jpdamoro na3	aplicación potencialmente no deseada	Win32/Toolbar.Iminent.E	Variante	Análisis a petición	13128 (20160804)	archivo	file:///C:/System Volume Information/_restore{1EBCD62A-D1BB-4755-A4D9-C81365DB059A}/RP485/A0109937.rbf	la acción seleccionada se ha retrasado hasta la finalización del análisis	no	no	ESET Remote Administrator	2016 mar. 4 12:23:54