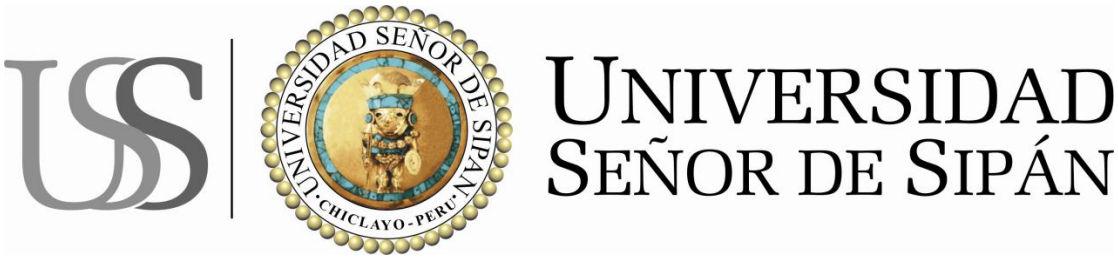

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

"IMPLEMENTACION DE PROTECCION PERIMETRAL CONTRA AMENAZAS DE MALWARE DESCONOCIDAS QUE NO ESTAN BASADAS EN FIRMAS EN ESSALUD A NIVEL NACIONAL"

AUTOR:

⇒ **BACH. Larry Edwin Anibal Riega Riega**

ASESOR:

ING. Miguel Ángel Vidaurre Flores.

PIMENTEL, NOVIEMBRE DEL 2015

RESUMEN

A pesar de las reiteradas recomendaciones de seguridad vertidas en las ferias de seguridad, foros tecnológicos, canales de distribución de mayoristas del ramo, oficiales de seguridad y organismos vinculados a la seguridad perimetral en ambientes de TI, se aprecia que un alto porcentaje del parque informático funcionando sobre la plataforma Windows se encuentra constantemente amenazado ante cualquier ataque proveniente de Internet debido a la falta del parche acumulativo de seguridad (SP3) para estaciones con Windows Xp y el SP1 para equipos con Windows Seven, con las consecuencias y riesgos que estas incidencias pueden ocasionar, como la pérdida de información, vulnerabilidades en el sistema operativo y la saturación de enlaces, que generan congestionamiento y degradación, en los sistemas de información, en claro perjuicio del usuario final.

Para ayudar a proteger la computadora de cualquier tipo de malware o amenaza proveniente de la nube es vital instalar las actualizaciones de seguridad desde el momento en que las mismas se encuentran disponibles o liberadas por el fabricante. La mejor manera de lograr lo señalado en el punto anterior es activar las actualizaciones automáticas, configurando el navegador para dicho propósito, entonces de ese modo se transfieren todos los parches de seguridad necesarios para dicho fin.

Es responsabilidad del Jefe Informático, que las recomendaciones de seguridad, contempladas también en la Norma Técnica Peruana, se encuentre implementada en la totalidad de estaciones con sistema operativo Windows. Este escenario de equipos vulnerables, facilita el ataque de códigos de malware (virus, gusanos, troyanos y todo aquel código que tiene como finalidad alterar el correcto funcionamiento de un equipo de cómputo), provenientes de múltiples fuentes y ocasionan que se saturen los enlaces de la red y daños a las estructuras de directorios de Windows, generando pérdida y daños a la información de nuestros clientes, estas estaciones pueden ser infiltradas y controladas remotamente por el atacante desde Internet, tomando el control del equipo y afectando seriamente nuestra Red Corporativa.

En el momento actual, la sola implementación de módulos antivirus estructurados en función a motores propietarios y la integración del archivo de firmas ha dejado en claro que solo puede reconocer hasta un máximo del 45% del total del vector de amenazas, la diferencia corresponde a amenazas de malware desconocidas o de nueva generación que están basadas en comportamiento y no en firmas como las amenazas tradicionales.

Palabras Clave

Malware, Seguridad Perimetral, Antivirus.

ABSTRACT
Despite repeated safety recommendations expressed in safety fairs, technology forums, distribution channels wholesalers in the industry, security officers and agencies related to perimeter security in IT environments, it is seen that a high percentage of computer equipment you operate on the Windows platform is constantly threatened against any attack from the Internet due to the lack of cumulative patch (SP3) supported on Windows XP and SP1 for Windows computers Seven, with the consequences and risks that these incidents could cause, such as loss of information, vulnerabilities in the operating system and saturation of bonds, which generate congestion and degradation, information systems, in clear prejudice to the end user.

To help protect your computer from any type of malware or threats from the cloud is vital to install security updates from the moment that they are available or released by the manufacturer. The best way to accomplish what is stated in the previous point is enable automatic updates, configuring the browser for that purpose, then that way all necessary security patches for this purpose are transferred. It is the responsibility of the Head Computer that safety recommendations also referred to the International Standard, is in place, in all stations with Windows operating system.

This scenario of vulnerable computers, facilitates the attack code malware (viruses, worms, Trojans and all that code that aims to disrupt the proper functioning of computer equipment), from multiple sources and cause the bonds are saturated network and damage to the Windows directory structures, generating loss and damage to customer information, these stations can be infiltrated and controlled remotely by the attacker from the Internet, taking control of the team and seriously affecting our corporate network.

At present, the mere implementation of structured modules based antivirus engines and integration owners signature file has made clear that it can only recognize up to 45% of total threat vector, the difference corresponds to threats unknown malware or new generation that are based on behavior rather than signatures as traditional threats, this major security breach creates a tunnel absent control vulnerabilities, detect and prevent malware attacks that threaten the integrity, confidentiality and availability of information systems and corporate communications, in fact if something is not known, it can't cope, it is for all the need to implement an additional layer of security based on behavior that complemented with traditional security solutions based on firms can cope with these threats as modern malware, which uses silos created specifically for cybercriminals and browsers purposes without patches as their penetration tools servers, the entire portfolio of products, web browsers and all applications running on the system operating are exploited by the authors of Malware, so that it can be installed on a computer and liaising Command and Control (C & C) can transfer information farms in the cloud and compromising confidential files, keys, or even download additional results unidentified malware on the network.

EsSalud required to have a Malware Detection System Next Generation, to protect the institution against cyber-attacks, particularly Malware, Botnets and other advanced persistent threats. This can be accomplished by passive detection in combination with active detection and blocking at the point of monitoring, administration of this technology will allow mentioned threats stop proactively new generation, have elements that provide remediation methods for infection and manage reports ability to take appropriate decisions to the security personnel information of EsSalud.

Keywords
Malware, Perimeter Security, Antivirus.