Seguridad Operativa

Alfonso Andrade Peña
Esp. Seguridad Informática Cohorte 14
Universidad Piloto de Colombia
Bogotá D.C
alfonsoandradep@hotmail.com

RESUMEN

Una de las mayores preocupaciones a nivel de tecnología informática es como cuidar, proteger o asegurar el mayor activo con el que se cuenta en los equipos, servidores, cintas, medios de almacenamiento como es la información.

El medio por el que circula la información, es por esto que la prioridad es como la respaldo, como evito que sea accedida por quienes no tienen los privilegios, y si logran obtener la información, como evitar que la lean, como evito que en el camino la intercepten y la modifiquen, este es el reto de hoy en día y esta es la fundamentación de este artículo.

Palabras Claves: Datos, Sistema Operativo, Seguridad, Criptografía, ISO/IEC 27002, Antivirus, Seguridad Perimetral.

ABSTRACT

One of the biggest concerns at the level of computer technology is how to care, protect and ensure the greatest asset that is counted on computers, servers, tapes, storage media such as information

The means by which information circulates, which is why the priority is as the backup, and avoid to be accessed by those who have no privileges, and if they get the information, how to avoid the read, as I stop in the way the intercept and modify, this is the challenge of today and this is the foundation of this article.

Keywords: Data, Operating System, Security, Cryptography, ISO / IEC 27002, Antivirus, Perimeter Security.

I. INTRODUCCIÓN

Proteger la Información y que medidas de seguridad debo tener en cuenta para proteger esta información tanto en la parte de sistema operativo como de transporte de la misma es la base de este estudio, dando algunos tips de cómo se fortalecer claves de seguridad y políticas sencillas para procurar hacer la plataforma tecnológica más segura practicando los principios de integridad, confidencialidad, disponibilidad y hasta de no repudio.

Siempre que utilizamos Internet para cualquier actividad, correo electrónico, navegación web, descarga de archivos, o cualquier otro servicio o aplicación, la comunicación entre los diferentes elementos de la red y nuestro propio ordenador requiere estar protegida, es por eso que se requiere asegurar los servidores, estaciones de trabajo y la forma como esta llega.

II. SISTEMA OPERATIVO.

Uno de los sistemas operativos más utilizados en las estaciones de trabajo y servidores es Microsoft Windows, al que se le han detectados numerosas vulnerabilidades, estas son detectadas y corregidas con actualizaciones de seguridad que se aplican periódicamente pero no es suficiente por lo que se deben tomar medidas adicionales para garantizar la confidencialidad, integridad y disponibilidad de la información.

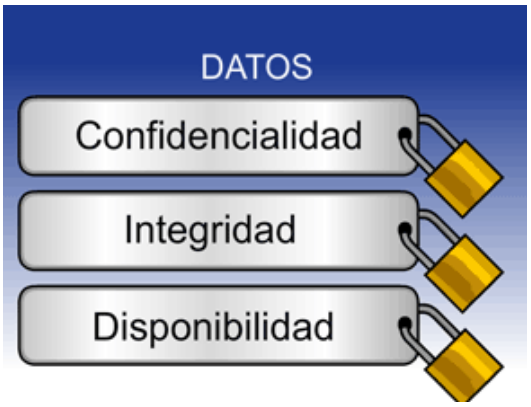

Figura 1. Principios de la Seguridad

A continuación se muestra cómo se puede proteger un computador y una red de computadores para evitar ser fácilmente atacados por un delincuente informático, las recomendaciones a seguir pueden ser muy triviales y el compendio de lo que siempre se dice y nunca se practica, un ejemplo claro es cuanto hace que cambie la clave de mi cuenta bancaria?, cuantas veces me han dicho que debo cambiar la

clave por lo menos una vez al mes?, cuantas veces me han dicho que la clave no debe ser 1234, pero siempre caemos en la pereza o costumbre de dejarle las cosas fáciles a los delincuentes.

III. SEGURIDAD BÁSICA

Uno de los mayores problemas son los errores de programación, más conocidos como bugs, estos son aprovechados por malware o virus que se encargan de causar daños dependiendo de la necesidad con la que se cuente, bien puede ser daño de información, sustraer información, saturar sistemas de almacenamiento o simplemente generar denegación de servicios.

Los consejos que se dan a continuación son generales y se pueden seguir independientemente del sistema operativo que se este utilizando. Concretamos estos consejos para el sistema operativo *Windows*, pero todo lo que se dice excepto algunas cosas puntuales son igualmente válidas para las versiones de Windows y otros sistemas operativos.

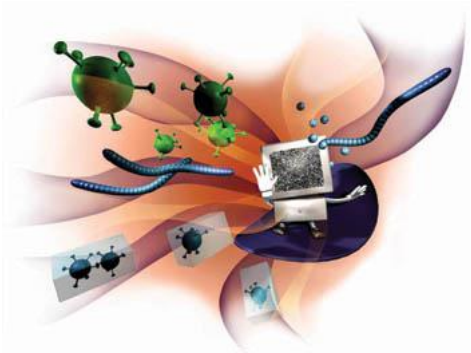

Figura 2. Protegiéndonos de los ataques

Actualizaciones de Windows: Microsoft libera el segundo martes de cada mes actualizaciones para sus productos, estos buscan cerrar los bugs que aprovechan los intrusos para poder crear cualquier tipo de problema informático, es por eso que debemos siempre mantener actualizados nuestros sistemas; para las empresas es muy importante contar con laboratorios en los que se hagan las pruebas y posteriormente se proceda a realizar el despliegue masivo utilizando siempre herramientas de distribución masiva; una económica y muy buena es WSUS, pero en el mercado se encuentran muchas pagas que igualmente cumplen con otras funciones.

Actualizaciones de otros Sistemas Operativo: Aunque hay sistemas operativos que no requieren un cronograma de implementación de parches mensuales como Unix, Linux, Mac, Solaris y algunos que se desprenden de Linux entre los más recientes para celulares y Tablet Android, si requieren actualizaciones de mejoras que de una u otra manera están cerrando y corrigiendo bugs que aunque no desestabilizan el sistema operativo si pueden afectar la Información que pasa por ellos.

Internet: Siempre que nos encontremos navegando por internet podemos ser víctimas, sin saberlo, de cambios en la configuración de nuestro navegador (Internet Explorer) y estamos expuestos a ser tomados por parte de spywares, código malicioso, gusanos, ficheros falsos al intercambiar archivos P2P o correos con dialers que modifican la configuración de la página de inicio, por lo que debemos siempre estar protegidos con antivirus y filtros de navegación que contengan estos ataques.

Políticas de Seguridad**:** Son muchas las normas de seguridad que se encuentran para llegar a un entorno seguro, hablando específicamente de ISO/IEC 27002 la versión de 2005 del estándar incluye las siguientes once secciones principales:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Gestión de Activos de Información.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de las Comunicaciones y Operaciones.
- Control de Accesos.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes en la Seguridad de la Información.
- Gestión de Continuidad del Negocio.
- Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la Información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

Password: En todas las normas certificables para la implementación de políticas de seguridad, el control principal está orientada hacia el aseguramiento a nivel de claves de acceso, la clave de seguridad a un computador o dominio debe ser cambiada mínimo cada 30 días, no debe ser un nombre, debe ser un compendio de números, letras y caracteres especiales no inferior a 8 caracteres, a continuación ejemplo de una clave segura, pueden utilizar un nombre o frase de la siguiente manera (Colombia2014 = C0l0mb1@/2O14 o

hoyesundiaperfecto H0y3sUnD1@P3rf3ct0&12), si es una clave administradora, definitivamente la mejor manera es hacerlo a través de un software generador de claves que siempre varia y no tiene ninguna relación como por ejemplo (H”3%-2nr).

Otros de los factores importantes a tener en cuenta son: el uso y manejo de los usuarios privilegiados, el manejo de los backups (respaldo de Información) y planes de contingencia.

Antivirus: Es un principal componente de la seguridad, que detecta y elimina software malicioso. Esta herramienta requiere estar actualizada, para que sea efectiva ante amenazas conocidas.

En el mercado se pueden encontrar distintas variedades de antivirus que permitan proteger los sistemas de seguridad, por lo tanto, para decidir cuál es el mejor se debe tener en cuenta el número de actualizaciones que libera, la estabilidad en el motor y el posicionamiento que tiene en el mercado.

Una buena herramienta de consulta es el cuadrante de Gartner, el cual determina quiénes son los mejores fabricantes que compiten en los principales mercados de tecnología, cómo están posicionados para ayudarle en el largo plazo. Esta herramienta sale de una investigación que ayuda en la culminación de la investigación en mercados específicos para ayudar a dar una posición ante la competencia mediante la aplicación de un tratamiento gráfico y un conjunto de criterios que ayudan a evaluar el posicionamiento y la prospectiva de cada fabricante. El cuadrante Mágico de Gartner ayuda a digerir rápidamente cómo los proveedores de tecnología se están comportando, a continuación un ejemplo de como se vería esta grafica para toma de decisiones: karpesky seria una opción al lado de symantec seguido por mcafee, sophos y trend micro cualquiera de estos cinco productos brindaría la mejor opción.

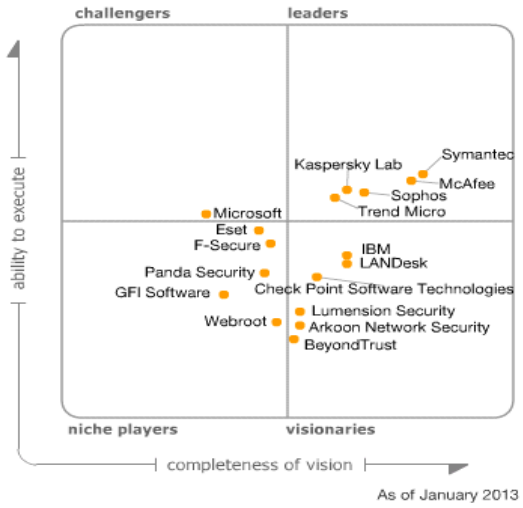

Figura 3. Cuadrante de Gartner

IV. FORTALECIENDO LA SEGURIDAD

Se cree que tener un perímetro seguro es solo tener un firewall, y colocarle unas políticas de bloqueo básico sin realizar un análisis de que quiero o que necesito para mi organización, hay una serie de herramientas que ayudan a fortalecer la puerta de entrada y salida de una organización.

Seguridad Perimetral: El perímetro de nuestra red siempre debe estar bien protegido y para lograrlo encontramos herramientas como son:

- Firewall: Un cortafuegos (*firewall* en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas
- Detección de Intrusos: Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusión Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos crackers, o de Script Kiddies que usan herramientas automáticas.
- Filtros de Contenido: un filtro de contenido (ver otros nombres) se refiere a un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web. El filtro de contenido determina qué contenido estará disponible en una máquina o red particular.
- Anti Spam: Un anti spam se conoce como método para prevenir el correo basura. Tanto los usuarios finales como los administradores de sistemas de correo electrónico utilizan diversas técnicas contra ello. Algunas de estas técnicas han sido incorporadas en productos, servicios y software para aliviar la carga que cae sobre usuarios y administradores
- Antivirus. Un antivirus de perímetro es el que se encarga de minimizar la carga hacia la red interna de trafico no deseado o posibles ataques, existen en el mercado antivirus en cajas o appliance, también se consigue software especializado y los firewall ya introducen algunos pequeños módulos dentro de sus soluciones.

Todos estos mecanismos de seguridad son independientes y cada uno de un fabricante o equipos hardware y software que cumplen con todas las funciones y son prácticos dependiendo del número de empleados, ancho de banda y proyección de crecimiento.

La seguridad perimetral debe estar acompañada de una buena política de seguridad, no sirve invertir dinero para instalar uno

o varios equipos de seguridad trabajando en modo de aprendizaje sin políticas claras de detección, acción y prevención.

V. CRIPTOGRAFÍA

La criptografía desciende del griego y significa escritura oculta, es el arte de poder cifrar y descifrar información mediante técnicas especiales y se utiliza para realizar un intercambio de mensajes que solo puedan ser leídos por las personas a las que va dirigido y que poseen la llave o medio para descifrarlos.

Los objetivos de la criptografía son los de mantener la confidencialidad para que el mensaje o documento no pueda ser visto o leído por personas no autorizadas, conservar la integridad asegurando que la información no pueda ser modificada por personas no autorizadas, mantener la autenticidad para que el remitente de un mensaje sea quien realmente dice ser y una parte muy importante es el manejo del no repudio debido a que se debe tener la seguridad de que no se deniega la recepción del envió.

Existe en criptografía variedad de documentos digitales que se usan para garantizar las propiedades de confidencialidad e integridad de la información, estos documentos son la integración de dos formas criptográficas que son simétricos y asimétricos. Al hacer esta integración se sacan las ventajas de los dos tipos de cifrado y se utilizan las mejores características de cada uno de los componentes, combinando rapidez del cifrado simétrico asociado a la facilidad de la administración de llaves del tipo de cifrado asimétrico.

El estado Colombiano mediante el Ministerio de tecnologías de la información y las comunicaciones MINTICs se encuentra divulgando y fortaleciendo el envío de información en forma segura; dando cumplimiento a las leyes y decretos que se encuentran establecidas dentro del marco jurídico contenido en nuestra constitución política nacional, por el cual la ley 527 de 1999 sobre la firma electrónica para el comercio electrónico contenido en el artículo 7, y regulado con el decreto 2364 de 2012. La ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales y se expide el **Decreto 1377 de 2013** "Por el cual se reglamenta parcialmente la ley que obliga a todas las entidades públicas y empresas privadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas. Conforme al Decreto Ley 019 de 2012, se suprime el requisito de imposición de huella dactilar en tinta, reemplazándolo por la obligación expuesta en el artículo 18, verificación de huella dactilar por medios electrónicos.

Existen en la actualidad tres entidades certificadoras que se encargan de emitir certificados, las empresa son Andes, GSE y Certicamara con las que se pueden solicitar servicios como certificado electrónico para subastas, correo, facturas, archivos, persona natural, persona jurídica, , firma digital y estampado cronológico entre otros.

VI. CONCLUSIONES

- Los ataques informáticos tienen una motivación propia, un empleado o ex empleado insatisfecho, un hacker, un virus, la parte económica, pero siempre buscan obtener algo que es la información.

- Los sistemas de información mas atractivos son las bases de datos del sector privado, el sector financiero pero dado que las organizaciones han mejorado la seguridad de sus infraestructuras de red, de escritorio y servidores, ha habido un cambio en el tipo de ataques hacia las aplicaciones.

- Debemos cerrar la puerta a posibles intrusiones teniendo una política de seguridad con prácticas sencillas que permitan ser divulgadas a los usuarios finales y ponerlas en práctica, la seguridad no solo es para los ingenieros o administradores, esta cubre todo el entorno de la empresa incluidos los accesos a Internet.

VII. REFERENCIAS

[1] NORMA ISO 27002.

[2] Imagen 1 tomada de la siguiente URL http://www.protegetuinformacion.com/imgs/temas_interes/7/tema_63.gif

[3] Imagen 2 tomada de la siguiente URL http://blog.interdominios.com/wp-content/uploads/2008/seguridad_red2.jpg

[4] http://es.wikipedia.org/wiki/ISO/IEC_27002

[5] http://portal.gse.com.co/

[6] http://web.certicamara.com/servicios

[7] https://www.andesscd.com.co/productos-mainmenu-68.html

[8] http://es.wikipedia.org/

[9] http://www.informaticamoderna.com/Sist_Ope.htm

[10] http://wiki.cenditel.gob.ve/wiki/Introducci%C3%B3n%20Al%20Cifrado

[11] http://es.wikipedia.org/wiki/Programa_esp%C3%ADa

[12] https://www.google.com.co/search?q=gartner+quadrant+antivirus+2013&tbm=isch&tbo=u&source=univ&sa=X&ei=wnT5UvntBYKnkQfMrIGACw&sqi=2&ved=0CDsQsAQ&biw=1440&bih=799#facrc=_&imgdii=_&imgrc=JXk5TLFFGgO2cM%253A%3BKlLJdf_Z7Bzx4M%3Bhttp%253A%252F%252Fwww.is4security.com%252Fmedia%252Fwysiwyg%252FMagic_Quadrant_for_Endpoint_Protection_Platforms_January_2013.png%3Bhttp%253A%252F%252Fwww.is4security.com%252Fquality.html%253F___store%253Ddefault%2526___from_store%253Dcesky%3B400%3B410
[13] http://www.gartner.com/technology/research/methodologies/research_mq.jsp