

Boletín de Asesoría Gerencial*

Seguridad en el Software Libre

No. 7 - 2008

Contenido Cerrar Imprimir Página anterior Página siguiente



ESPIÑEIRA, SHELDON Y ASOCIADOS

Firma miembro de

PRICEWATERHOUSECOOPERS 

Contenido

Haga click en los enlaces para navegar a través del documento



Haga click en los enlaces para llegar directamente a cada sección

- ▶ Seguridad en el Software Libre

- ▶ Definición de software libre

- ▶ Licencias de software libre

- ▶ Ventajas y desventajas del software libre

- ▶ Seguridad por oscuridad vs. Seguridad por visibilidad

- ▶ Soluciones de seguridad con software libre

- ▶ Factores críticos de éxito

- ▶ Conclusión

- ▶ Créditos

Boletín de Asesoría Gerencial

Seguridad en el Software Libre



Seguridad en el Software Libre

El uso del software libre es una tendencia que busca mostrarse como una alternativa viable para organizaciones y los usuarios comunes, afianzado en su promesa de disminución de costos, facilidad de acceso, adaptación a necesidades particulares y apoyo al usuario mediante foros de ayuda en Internet.

Aunque los aspectos antes mencionados en primera instancia lucen atractivos, es necesario incorporar en este análisis el tema de la seguridad de la información.

Definición de software libre

El concepto de software libre radica en la capacidad que tienen los usuarios para ejecutar, copiar, modificar, mejorar y redistribuir libremente dicho software. Bajo la filosofía de “libertad” que ha dado origen al movimiento, han surgido cuatro niveles:

1. Ejecutar el software para cualquier propósito
2. Estudiar y modificar el programa para adaptarlo a ciertas necesidades
3. Copiar y distribuir el programa
4. Realizar y publicar mejoras para el beneficio de terceros

En las opciones b y d antes mencionadas, los usuarios tienen acceso al código fuente. Este tipo de software es conocido hoy en día como “Open Source”.

En contraposición, la redistribución o modificación del software propietario no se puede realizar o se necesita autorización para ello, y el usuario generalmente no tiene acceso al código fuente.

Boletín de Asesoría Gerencial

Seguridad en el Software Libre



Licencias de software libre

La licencia más comúnmente utilizada es la Licencia Pública General de GNU (GNU GPL), pero también se utilizan otras licencias no compatibles con la GPL de software libre, dentro de las cuales se encuentran:

- Licencia Pública General de Affero.
- La Licencia Pública Arphic.
- La licencia BSD original.
- La licencia de OpenSSL.
- La Licencia Libre Académica (AFL), versión 1.1.
- La Licencia de Software Abierto, versión 1.0.
- La Licencia de Apache, versión 1.0, 1.1 y 2.0.
- La Licencia Pública de Zope versión 1.

Ventajas y desventajas del software libre

A pesar de que el uso de software libre está en constante crecimiento, junto con el mismo aumenta la exposición y el debate sobre sus ventajas y desventajas. El conocimiento de estas características es un factor importante a la hora de elegir el tipo de software libre que mejor se adapta a la implementación que se quiere realizar.

Ventajas

- Derecho de uso sin incurrir en costo alguno.
- Acceso al diseño del software, lo que permite conocer al detalle lo que se está instalando, así como agregar mejoras y funciones.
- Es modificable, si el software tiene limitaciones o no es adecuado para una tarea, es posible adaptarlo a necesidades específicas y redistribuirlo libremente.
- Es de libre distribución, cualquier persona puede regalarlo, venderlo o prestarlo.

- Tiende a ser eficiente y robusto en diferentes entornos, debido a la colaboración de los usuarios que lo modifican, buscando optimización y mejoras.
- Tiende a ser utilizado en diversos escenarios: la gente que contribuye tiene muchas necesidades diferentes y esto hace que el software esté adaptado a una cantidad más grande de problemas.

Desventajas

- La curva de aprendizaje es mayor.
- El software libre no tiene garantía proveniente del autor.
- Se necesita dedicar recursos a la reparación de erratas.
- No existe una compañía única que respalde el soporte.
- Las interfaces amigables con el usuario (GUI) y la multimedia se encuentran en un continuo proceso de estabilización

Boletín de Asesoría Gerencial

Seguridad en el Software Libre



Ventajas y desventajas del software libre (*continuación*)

- La mayoría de la configuración de hardware no es intuitiva, se requieren conocimientos previos acerca del funcionamiento del sistema operativo y fundamentos del equipo a conectar para lograr un funcionamiento adecuado.
- Únicamente los proyectos importantes y de trayectoria tienen buen soporte, tanto de los desarrolladores como de los usuarios; sin embargo existen muchos proyectos más pequeños y recientes que carecen del compromiso necesario por parte de sus usuarios o desarrolladores para que sean implementados de manera confiable.
- La diversidad de distribuciones, métodos de empaquetamiento, licencias de uso, herramientas con un mismo fin, etc., pueden crear confusión en cierto número de personas.

Seguridad por oscuridad vs. Seguridad por visibilidad

La seguridad por oscuridad es la filosofía bajo la cual se expresa que cualquier software puede ser seguro mientras su funcionamiento interno y la seguridad de éste no se divulgue fuera de su grupo de desarrollo e implementación. Para esto se aplican mecanismos como ocultar contraseñas en archivos binarios y cerrar el acceso a cualquier elemento relacionado con el código fuente.

Esta característica del software propietario hace que las vulnerabilidades de éste no sean públicas, quedando pendientes las emisiones de correcciones y actualizaciones por parte del fabricante.

La seguridad por visibilidad se basa en la divulgación de las vulnerabilidades que son detectadas y solucionadas como consecuencia del gran volumen de usuarios que tienen acceso al código fuente del software o que lo usan sin restricciones.

No se puede plantear que efectivamente el software cerrado o propietario sea menos seguro que el software libre, o viceversa. La seguridad de la plataforma va a depender de un plan completo de seguridad que evalúe todos los elementos que la componen.

Boletín de Asesoría Gerencial

Seguridad en el Software Libre



Soluciones de seguridad con software libre

En el mercado existen diversas soluciones de seguridad basadas en software libre, cuyo uso comienza a crecer como alternativa a aplicaciones de software propietario.

En el caso de la seguridad para usuarios remotos existen herramientas que permiten cifrar la información contenida en los dispositivos de almacenamiento (TrueCrypt) y para administración de conexiones remotas (OpenVPN). También se puede mencionar GMF, una herramienta web para la gestión diaria de las PYMES. Con esta herramienta no es necesario instalar ninguna aplicación adicional en las estaciones de trabajo de los usuarios y es accesible, mediante un sistema de permisos, para los usuarios remotos que se conectan a través de Internet.

En lo relacionado a la seguridad perimetral se encuentran disponibles firewalls que permiten filtrar paquetes mediante la definición de políticas, monitoreo del tráfico y honeypots.

Entre estas herramientas se encuentra “TigerWeb”, que se encarga de realizar análisis de seguridad perimetral en redes IP, mediante la ejecución de pruebas sobre máquinas que disponen de una dirección IP externa, buscando potenciales vulnerabilidades que puedan ser utilizadas por usuarios no autorizados para acceder, corromper, destruir o impedir el acceso a dichos sistemas. Así mismo, genera un informe con los resultados obtenidos. Otras soluciones destacadas son IPTables (Firewall), Snort (Detección de intrusos) y Squid (Proxy).

En cuanto a seguridad de servidores, el catálogo disponible de herramientas de software libre incluye, entre otras, a Nessus (Detección de vulnerabilidades), OpenSSH (Sesiones seguras), así como una variedad de soluciones para manejo de certificados digitales, monitoreo de tráfico, detección de software maligno y de correo SPAM.

Boletín de Asesoría Gerencial

Seguridad en el Software Libre

Equilibrio entre software libre y software propietario

Hoy en día, resulta difícil implementar una plataforma basada totalmente en software libre que satisfaga las necesidades de las organizaciones, lo cual conlleva a la necesidad de una convivencia entre el software libre y el software propietario.

El aspecto fundamental a la hora de tomar decisiones relacionadas con el software a adquirir es la necesidad de implementar soluciones que persigan la satisfacción de los requerimientos de la organización, en base a los objetivos, las estrategias y las particularidades del negocio. Asimismo, se deben comparar las opciones considerando tanto aspectos tangibles como intangibles, y tomar en cuenta que las soluciones consolidadas ofrecen mayores garantías que las soluciones aisladas.

Factores críticos de éxito

Adquirir un software representa sólo el primer paso hacia una implementación exitosa, también es importante que la organización tome acciones en relación a:

- Adiestramiento: brindarle la información y entrenamiento a los usuarios sobre cómo usar el software y cómo abordar la seguridad en cada una de sus labores, disminuye la dependencia operativa a terceros, sin incurrir en problemas de confidencialidad, integridad y disponibilidad de la información.
- Entendimiento del negocio: como se planteó en la sección anterior se debe estudiar cómo apoyan las estrategias y se alinean con los objetivos del negocio; sólo se debe efectuar una adquisición de un software si es requerido actualmente y para cumplir con el plan

estratégico de TI de la organización. Cabe destacar que existen múltiples productos para software libre que ejecutan funciones similares, e incluso puede ser subproductos de otros, por lo que se debe reforzar el proceso de selección para evitar costos innecesarios.

- Entendimiento de usuarios finales: es importante considerar el impacto cultural que puede tener en los usuarios finales la implementación del nuevo software y determinar un plan de acción para facilitar la adaptación de los usuarios al cambio.
- Considerar las necesidades que tendrá la organización y los clientes en el futuro para desarrollar la infraestructura tecnología adecuada.

Boletín de Asesoría Gerencial

Seguridad en el Software Libre



Conclusión

El software libre es una tendencia en crecimiento, que trata de forma distinta las facetas del software: desarrollo, comercialización, distribución y uso. También brinda capacidades de modificación que permite realizar adaptaciones, actualizaciones, mejoras y diversificaciones, libre distribución de copias, contemplando aspectos de seguridad, privacidad, colaboración, competitividad y eficiencia.

Persiste la controversia sobre la seguridad del software libre frente al software con licencia: Un procedimiento utilizado con frecuencia a la hora de evaluar qué tan seguro puede ser una solución de software es investigar sobre las fallas de seguridad que han sido reportadas y si éstas han sido solucionadas adecuadamente, sin embargo este esquema es susceptible a la interpretación de quienes analizan y consolidan esta información, pudiendo incluso ser calificados de

estudios financiados para apoyar una u otra tendencia. Así mismo, la adquisición de cualquier elemento debe ir dentro de un plan que contemple todos los elementos relacionados.

En todo caso, el futuro se avizora hacia un ambiente de coexistencia de software propietario y libre, particularmente en grandes organizaciones y el sector gobierno. Bajo este escenario, prevalece la necesidad de un enfoque de gestión integral de la seguridad de información, que incorpore a lo largo del ciclo de vida del software la identificación, valoración, aplicación de medidas de control, monitoreo y respuesta a incidentes, permitiendo una reducción efectiva del riesgo en la utilización de la tecnología de información.

Boletín de Asesoría Gerencial

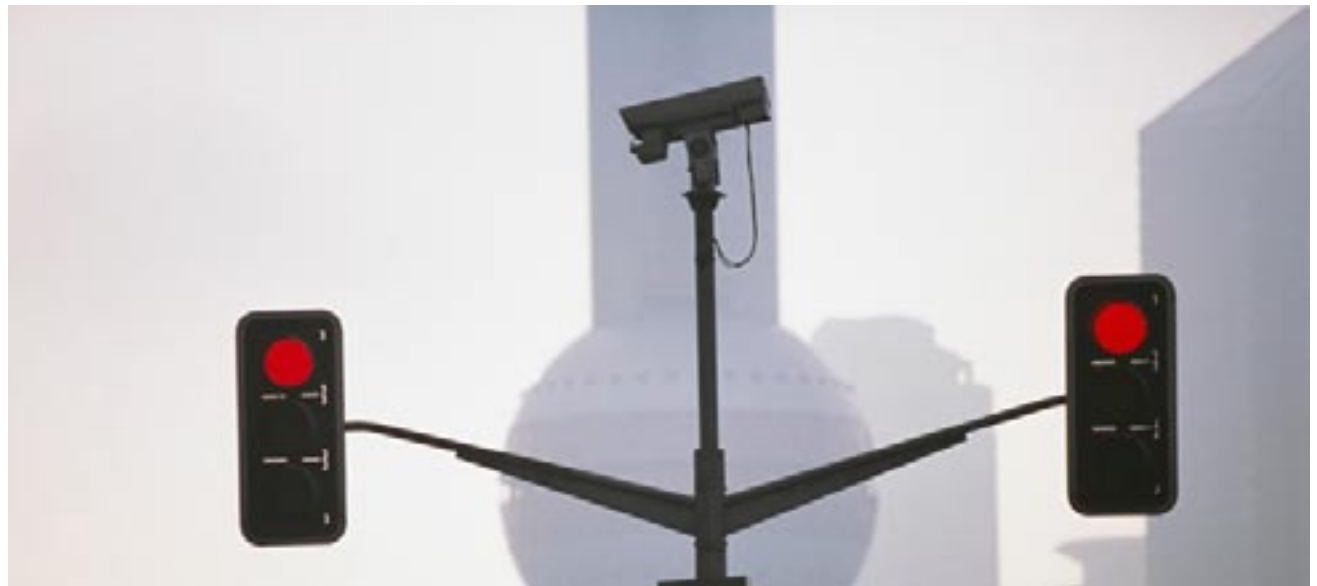
Seguridad en el Software Libre

Si desea suscribirse haga click en la barra

El Boletín Asesoría Gerencial es publicado mensualmente por la Línea de Servicios de Asesoría Gerencial (Advisory) de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. *connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados
Depósito Legal pp 1999-03CS141
Teléfono master: (58-212) 700 6666



© 2008. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3