Adecuándose a la norma ISO/IEC 1799 mediante software libre [*]

Jose Fernando Carvajal Vión
Grupo de Interés en Seguridad de ATI (ATI-GISI)
<carvaco@ati.es>
Javier Fernández-Sanguino Peña
Grupo de Interés en Seguridad de ATI (ATI-GISI)
<jfs@computer.org>

28 de octubre de 2002

Resumen

Este artículo muestra la forma de adecuar a la norma ISO/IEC 17999 un sistema de información implementado en un servidor cuyo software de sistema operativo se basa en alguna alternativa de software Libre y código abierto. La utilización de una distribución Debian GNU/Linux sirve como base a la que añadir las utilidades y paquetes necesarios para conseguir el objetivo.

Índice

1. Introducción

De forma general para mantener la seguridad de los activos de información se deben preservar las características siguientes [1].

1. Confidencialidad: sólo el personal o equipos autorizados pueden acceder a la información.

2. Integridad: la información y sus métodos de proceso son exactos y completos.

3. Disponibilidad: los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando se requieran.

La implantación de la seguridad de la información, en la medida de lo posible, se consigue mediante un conjunto adecuado controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones software. Estas medidas de control sirven para asegurar que se cumplen los objetivos específicos de seguridad de la Organización.

En el campo normativo voluntario de la gestión de la seguridad de las TI existen actualmente, como más relevantes, las normas siguientes:

- La norma ISO/IEC 17799 [2] que ofrece las recomendaciones para realizar la gestión de la seguridad de la información, las versión española de esta norma es la UNE 717799 [116].

- La norma multiparte ISO/IEC 13335 [117,118,119,120,121] conocidas como las GMITS donde se recogen las etapas del ciclo de gestión de la seguridad proporcionando orientaciones organizativas y técnicas, la versión española de esta norma multiparte es la UNE 71501 IN [122,123,124].

- Generalmente cada Organización en base a los riesgos a que esté expuesta y los aspectos intrínsecos de su funcionamiento, define e implanta un Sistema *propio* para realizar de forma estructurada, sistemática y metódica la gestión de la seguridad de TI. Para algunas organizaciones puede ser orientativa la norma Británica BS-7799-2 [3], la cual fija requisitos para establecer, implementar y mantener un Sistema de gestión de la seguridad de los sistemas de información (ISMS: Information Systems Management System).

Aquellas organizaciones que quieran ser conformes a la norma BS-7799-2 deberán cumplir estrictamente los requisitos según se indican en su texto. Dada la riqueza de variantes presentes en el mundo real, para algunas organizaciones la norma resulta meramente orientativa.

Algunas empresas podrán considerar importante la adecuación a una norma para obtener la certificación correspondiente porque su proceso de negocio (o clientes) lo demanden. Sin embargo, aunque ésto pueda ser el caso para otras normas ISO (como la ISO 9000) no lo es tanto para la norma ISO/IEC 17799. ¿Por qué, entonces, puede ser necesario adecuarse a una norma como el ISO/IEC 17799? La utilización

de una norma de seguridad permite cerciorarse de que se cubren todos los aspectos de seguridad que debe abordar una organización, desde la especificación de una política de seguridad a la definición de necesidades de seguridad física o de recuperación de desastres. Claramente, una organización puede abogar por definir su política de seguridad y realizar su implementación sin seguir ninguna norma. El beneficio de utilizar una norma es el de acceder al conocimiento de expertos reflejado en una guía accesible a cualquier responsable de seguridad.

2. Objetivo y Asunciones

Nuestro objetivo es realizar una identificación de aquellos puntos de la norma ISO/IEC 17799 que pueden ser cumplidos por toda instalación de un servidor basado en Debian GNU/Linux, por tanto nos dirigimos a la implementación de los controles de seguridad según las necesidades de la organización o partes de ésta indicando que herramientas pueden utilizarse para implementar cada control concreto. Algunas de las herramientas (la gran mayoría como se verá) estarán proporcionadas como software libre dentro del software que forma parte de la distribución mientras que otras, también software libre, habrán de ser obtenidas de otras fuentes e instaladas en éste.

En este artículo supondremos en todo momento la existencia de unas necesidades de seguridad identificadas, evaluadas y establecidas dentro de una organización o empresa conforme a sus necesidades.

No obstante, para pequeñas y medianas empresas (PYMES), se podrían implementar las medidas de seguridad dictadas por la Norma ISO/IEC 17799 en sus servidores utilizando un sistema operativo Debian GNU/Linux 3.0 *woody* como referencia [4] y configurándolo con las herramientas y utilidades necesarias. Adecuándolo así a las medidas de control dictadas por ésta que permitan cubrir razonablemente los requisitos de seguridad específicos para cada caso.

Tomamos la versión estable de Debian como referencia por que es, a nuestro juicio, la que mejor se adapta a la filosofía del software libre [5] (también llamado en algunos casos código abierto [6]). Ejemplos de instalación de servidores puede consultarse por toda la Red Internet.

Como marco de referencia debemos presuponer que nos encontramos dentro de una organización o empresa con una política de seguridad definida o que al menos toma como base el código de buenas prácticas [2]. Esto nos permite obviar la parte organizativa de la norma y centrarnos en la parte de implementación técnica de la misma; intentando en todo momento equiparar las especificaciones de la norma en su aspecto operativo y no en el organizativo.

La idea central es, pues, determinar en qué puntos un sistema operativo GNU/Linux dotado de los programas de utilidad adecuadas puede llegar a cumplir y ser certificado en la norma. No se debe considerar una cortapisa el hecho de que, actualmente, ninguna de las distintas distribuciones del sistema operativo GNU/Linux se hayen certificadas en el ámbito de la seguridad. Uno de estos estándares bien podría ser el conocido como *Common Criteria*). En este análisis no se va a incidir en los aspec-

tos que pueda cubrir el sistema operativo GNU/Linux con respecto a los elementos de los Perfiles de Protección de Sistemas Operativos de dicho estándar (perfiles de protección que, por otro lado, aún están en fase de borrador).

En el análisis de la norma se marcará como *Política* aquellos controles que no puedan limitarse a una aplicación software concreta y que por el contrario deben implementarse como un conjunto de medidas software y/o medidas organizativas. En algunos de estos puntos podrán indicarse las referencias a los documentos y/o *HowTos* (documentos descriptivos de la utilización de algún elemento en software, a veces traducido como *Comos*) adecuados al caso y que pueden ser utilizados para crear los procedimientos organizativos que permitan cumplir ese control.

En cuanto al hardware del servidor mencionar que partimos del supuesto de un criterio de selección basado en las especificaciones actuales de hardware que pueden encontrarse en un PC de altas prestaciones del mercado de consumo cuyo rango de precio se encuentre dentro del coste aceptable para una pequeña empresa. Evidentemente, algunos de los controles contemplados en la norma se han de implementar mediante mecanismos físicos. La discusión de los mecanismos físicos de protección de los recursos salen fuera del ámbito de este trabajo.

3. Cumplimiento de la Norma ISO/IEC 17799 en GNU/Linux

En la tabla adjunta se relacionan los objetivos de control y los controles con marcado carácter operativo que pueden ser proporcionados bien por el núcleo del sistema operativo (Linux) o bien por los programas de utilidad adecuados. Por este motivo los puntos especificados en los apartados 3.1.1 a 8.1 se han obviado ya que entendemos que todos ellos deberían estar implementados mediante los procedimientos adecuados según el código de buenas prácticas [2] y ser realizados mediante procesos manuales o más o menos automatizados. Como ejemplo de este tipo de proceso podríamos usar el punto 6.3.1 *Notificación de Incidentes de Seguridad* en el que parte del mismo puede ser implementado mediante un sistema de detección de integridad como tripwire [8], un sistema de detección de intrusos como Snort [9], un sistema de análisis de ficheros como logcheck [125] un servicio de comunicación vía mail o GSM/SMS.

La tabla muestra la información recogida en el análisis realizado de forma conjunta a este trabajo. En aquellos elementos de control que disponen de herramientas de software libre para su implementación. No se ha hecho distinción de las herramientas proporcionadas dentro de la distribución Debian GNU/Linux (la mayoría) y las que no lo están. Esto es así porque, debido al ritmo de crecimiento de la distribución (actualmente consta de más de 3 Gbs de software, la versión anterior ofrecía más de 2 Gbs de sofware libre) es más que probable que aquellas herramientas de software libre útiles para el sistema serán incluidas en siguientes revisiones.

Se pueden consultar fuentes de información adicionales [10] que enlazan con documentación y utilidades software que pueden usarse para establecer los controles de seguridad previsto en la norma.

4. Conclusiones

Desde el punto de vista de una pequeña empresa aplicar las medidas técnicas para cumplir con la norma BS 7799-2 sería una tarea que cualquier administrador de seguridad podría llevar a cabo sin mayor dificultades a la vista de este artículo. Desgraciadamente las pequeñas empresas suelen carecer de una política de seguridad formalmente establecida (aunque también carecen de ésta política muchas empresas de mayor envergadura); sin embargo en el mejor de los casos impera el sentido común.

En los casos de empresa medianas y grandes es fundamental el establecimiento formal del entorno "político"de seguridad mediante la difusión y seguimiento de las buenas prácticas establecidas por la ISO/IEC 17799:2000.

En cualquier caso, es importante destacar el hecho de que las medidas de seguridad puedan implementarse con software libre, como demuestra el análisis realizado. Esto permite llevar a cabo implementaciones de la política de seguridad sin que sea necesario considerar el coste del software (dado que éste es software libre) y sin que aparezcan problemas de escalabilidad (no existiendo pago por licencias en función del número de equipos). El primero de los problemas es al que habitualmente se enfrentan las pequeñas empresas por el elevado coste del software asociado a la seguridad, el segundo de los problemas es también común en empresas grandes debido al elevado número de sistemas a asegurar.

El software libre ofrece, por tanto, una solución válida al entorno de seguridad de cualquier organización permitiendo la adecuación e implementación de políticas de seguridad basadas en estándares internacionales.

5. Referencias

[1] Stallings Willian , / Introduction Cryptography and network security: principles and practice. Chapter 1, 2nd Ed. Edit. Prentice Hall New Jersey (USA),1999, pp. 5.

[2] Information Security Management, Code of Practice for Information Security Management. International Standard ISO/IEC 17799:2000.

[3] Information Security Management. Part 2 Specification for information security management systems. Draft BS 7799-2:2002.

[4] Proyecto Debian. Paquetes y Documentación 1 julio 2002. <http://www.debian.org> [Consulta: 5 julio 2002].

[5] FSF (Free software Foundation). La definición de Software Libre 10 mayo 2002 <http://www.gnu.org/philosophy/free-sw.es.html> [Consulta: 5 julio 2002].

[6] Open Source Initiative. The Open Source Definition [en línea] . <http://www.opensource.org/do > [Consulta: 5 julio 2002].

[12] Harris, Tony. Koehntopp, Kristian. Linux Partition HOWTO.Ver 3.3 10 July 2001 <http://www.tldp.org/HOWTO/mini/Partition/> [Consulta: 6 julio 2002].

[13] HotScripts.com. Script para Manejo de Usuarios en Perl [en línea] <http://www.hotscripts.com [Consulta: 6 julio 2002].

[21] Bogar, Lisa. SUID, SGID and fix-modes Suid, Gid, [online]. <http://www.homepage.montana.
xuser/051602/SUID.html> [Consulta: 6 julio 2002].

[32] Wolfe Wiliam, Miller Donna . Secure Audit for Linux http://secureaudit.sourceforge.net/
[Consulta: 6 julio 2002].

[33] McIntyre Jim. Mastering system accounting in Linux. Ver Nov 22, 2000
<http://mycomputerstore.ca/llsa.html> [Consulta: 6 julio 2002]

[50] IBM Corporation. IBM zseries <http://www-1.ibm.com/servers/eserver/zseries/900.html>
[Consulta: 6 julio 2002]

[52] Tallyman <http://Tallyman.akopia.com> [Consulta: 6 julio 2002]

[54] Mutz, Marc. Encryption HOWTO Ver:0.2.2, 04 Oct 2000 <http://encryptionhowto.sourceforge
HOWTO.html#toc6 > [Consulta: 6 julio 2002]

[55] Tzeck, Doobee. R. Encrypting your Disks with Linux Ver 25 Oct 1999.
<http://koeln.ccc.de/~drt/crypto/linux-disk.html > [Consulta: 6 julio 2002]

[59] Reelsen, Alexander. Fernández-Sanguino Peña, Javier. Debian Security Manual http://www.debian.org/doc/manuals/securing-debian-howto/index.en.html> [Consulta: 6 julio 2002]

[63] Dreier, Roland. Johnson, Rob. Bhattacharyya, Bina. Gphone <http://gphone.sourceforge.net/
[Consulta: 6 julio 2002]

[64] Jackson, Michael H. Linux Shadow Password Howto. Ver: .3, 3 Abril 1996
<http://www.linuxdoc.org/HOWTO/Shadow-Password-HOWTO.html> [Consulta:
6 julio 2002]

[65] Morgan, Andrew G. The Linux-PAM System Administrators' Guide Ver:
v0.75 18 Marzo 2001 <http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html>
[Consulta: 6 julio 2002]

[66] Rsbac.org. RSBAC: Rule Set Based Access Control for Linux <http://www.rsbac.org/
> [Consulta: 6 julio 2002]

[67] Smartcard en Linux <http://www.linuxnet.com/> [Consulta: 6 julio 2002]

[71] Forbes, Liam. Sudo and SSH: A Scheme for Controlling Administrator Privileges and System Account. Ver: Junio 2001 <http://rr.sans.org/authentic/sudo.php>
[Consulta: 6 julio 2002]

[72] Muffett, Alec. FAQ for Crack v5.0a. Ver: 21 Marzo 2001 <http://www.users.dircon.co.uk/~cryp
faq.html> [Consulta: 6 julio 2002]

[89] Drake, Joshua. Linux Networking HOWTO.Ver: 1.7.0 <http://www.tldp.org/HOWTO/Net-
HOWTO/index.html> [Consulta: 6 julio 2002]

[90] Gilmore, John. Spencer, Henry. Linux FreeSWAN (Ipsec) <http://www.freeswan.org/>
[Consulta: 6 julio 2002]

[91] Foucher Laurent, Latu Philippe, Mallard Thierry, Quenec'hdu Yannick. Linux Advanced Routing & Traffic Control HOWTO Ver 1.0.0 8 Julio 2002 <http://lartc.org/>
[Consulta: 6 julio 2002]

[92] Kuznetsov, Alexey N. Iproute2: IP Command Reference <http://defiant.coinet.com/iproute2/
cref/> [Consulta: 6 julio 2002]

[93] Light-Williams, Corwin. Drake Joshua. Linux PPP Howto. . <http://www.ibiblio.org/mdw/H
HOWTO/index.html> [Consulta: 6 julio 2002]

[94] Controlling Suid Root Programs <http://www.dpo.uab.edu/~grapeape/suid.html>
[Consulta: 6 julio 2002]

[95] Akin, Thomas. Dangers of SUID Shell Scripts <http://www.samag.com/documents/s=1149/sa
[Consulta: 6 julio 2002]
[96] Bishop, Matt. Secure Suid programs <http://nob.cs.ucdavis.edu/~bishop/secprog/index.html>
[Consulta: 6 julio 2002]
[97] Counterpane.com. Log Analysis Resources <http://www.counterpane.com/log-analysis.html> [Consulta: 6 julio 2002]
[98] McDonald, Andrew D. StegFS - A Steganographic File System for Linux http://www.mcdonald.org.uk/StegFS/> [Consulta: 6 julio 2002]
[99] Mills, Dave. Network Time Protocol (NTP) <http://www.eecis.udel.edu/~ntp/>
[Consulta: 6 julio 2002]
[100] Wilson, Matthew D. VPN Howto Ver: Revision 2.0 30 Mayo 2002 <http://www.tldp.org/HOW
HOWTO/> [Consulta: 6 julio 2002]
[102] Davey, Dave. GSM Mobile Phones and Linux <http://www.physiol.usyd.edu.au/daved/linux/
modem.html > [Consulta: 6 julio 2002]
[106] Loscocco, Peter. Smalley, Stephen. Integrating Flexible Support for Security Policies into the Linux Operating System <http://www.nsa.gov/selinux/doc/slinux.pdf
> [Consulta: 6 julio 2002]
[109] Wheeler, David A. Secure Programming for Linux and Unix HOWTO Ver: 2.962, 12 Mazo 2002 <http://www.tldp.org/HOWTO/Secure-Programs-HOWTO/>
[Consulta: 6 julio 2002]
[116] UNE 717799-1:2002 IN Código de buenas prácticas para la Gestión de la Seguridad de la Información
[117] ISO/IEC 13335-1 IT- Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for managing and planning IT security
[118] ISO/IEC 13335-2 IT- Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security
[119] ISO/IEC 13335-3 IT- Security techniques - Guidelines for the management of IT security - Part 3: Techniques for the management of IT security
[120] ISO/IEC 13335-4 IT- Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards
[121] ISO/IEC 13335-5 IT- Security techniques - Guidelines for the management of IT security - Part 5: Management guidance on network security
[122] UNE 71501-1 IN Parte 1: Conceptos y modelos para la seguridad de TI
[123] UNE 71501-2 IN Parte 2: Gestión y planificación de la seguridad de TI
[124] UNE 71501-3 IN Parte 3: Técnicas para la gestión de la seguridad de TI

6. Referencias de herramientas

[8] Tripwire.org. Tripwire Open Source, Linux Edition http://www.tripwire.org/
[Consulta: 5 julio 2002].
[9] Caswell, Brian y Roesch, Marty. Snort: The Open Source Network Intrusion Detection System, 5 julio 2002 <http://www.snort.org/> [Consulta: 5 julio 2002].
[10] Linux-Consulting. IDS: Intrusion Detection Systems.30 mayo 2002. <http://www.linux-sec.net/IDS/ > [Consulta: 5 julio 2002].

[11] Yoshinori K. Okuji. Gnu Grub. . 4 julio 2002. <http://www.gnu.org/software/grub/ > [Consulta: 6 julio 2002].

[14] Oslo University College. Cfengine a configuration engine. <http://www.cfengine.org/> [Consulta: 6 julio 2002].

[15] BB4 Technologies. Big Brother. <http://www.bb4.com/> [Consulta: 6 julio 2002].

[16] Trocki, Jim. Mon: Service Monitoring Daemon. <http://www.kernel.org/software/mon/> [Consulta: 6 julio 2002].

[17] PandaSoftware.es. Panda Antivirus para Linux. [online]. <http://www.pandasoftware.es/es/li [Consulta: 6 julio 2002].

[18] OpenAntivirus.org. The Open Antivirus Project. [online]. <http://www.openantivirus.org> [Consulta: 6 julio 2002].

[19] Kapersky Lab Int. Kaspersky Anti-Virus for Linux Systems. [online]. <http://www.kaspersky.c [Consulta: 6 julio 2002].

[20] GeCAD Software. RAV Reliable Antivirus [online]. <http://www.ravantivirus.com > [Consulta: 6 julio 2002].

[22] Samhain Labs. Samhain. [online].<http://samhain.sourceforge.net/> [Consulta: 6 julio 2002].

[23] Lehti, Rami. Virolainen, Pablo. AIDE Advanced Intrusion Detection Environment. [online]. <http://www.cs.tut.fi/~rammer/aide.html> [Consulta: 6 julio 2002].

[24] University of Maryland at College Park. Amanda: The Advanced Maryland Automatic Network Disk Archiver. 10 junio 2002. <http://www.amanda.org/> [Consulta: 6 julio 2002].

[25] Arkeia. Arkeia Entreprise Network Backup. <http://www.arkeia.com> [Consulta: 6 julio 2002].

[26] Hülswitt, Stefan. CDBackup. <http://www.muempf.de/cdbackup.html> [Consulta: 6 julio 2002].

[27] Gignac, John-Paul. Volokhov. Mike M. cdbkup <http://cdbkup.sourceforge.net/ >[Consulta: 6 julio 2002].

[28] BalaBit IT Ltd. Syslog-ng. <http://www.balabit.hu/en/downloads/syslog-ng/> [Consulta: 6 julio 2002].

[29] Event log, 2002 Event Logging . <http://evlog.sourceforge.net/linuxEvlog.html> [Consulta: 6 julio 2002].

[30] Karim Yaghmour et al. The Linux Trace Toolkit. . <http://www.opersys.com/LTT/index.html [Consulta: 6 julio 2002].

[31] Linux Kernel Audit daemon,. 2002 <http://www.hert.org/projects/linux/auditd/ >[Consulta: 6 julio 2002].

[34] linuxvirtualserver.org. Linux Virtual Server Project [en línea] <http://www.linuxvirtualserver. [Consulta: 6 julio 2002]

[35] Oetiker, Tobias.Rand, Dave et al. MRTG: Multi Router Traffic Grapher <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/> [Consulta: 6 julio 2002]

[36] Psionic Technologies Inc. TriSentry <http://www.psionic.com/products/trisentry.html> [Consulta: 6 julio 2002]

[37] Deraison Renaud, Hrycaj, Jordan. Nessus <http://www.nessus.org/> [Consulta: 6 julio 2002]

[38] Fyodor. Nmap <http://www.insecure.org/nmap/> [Consulta: 6 julio 2002],

[39] Venema Wietse (The Indiana University Web site). Tcpwrappers <http://www.uwsg.indiana.e [Consulta: 6 julio 2002]

[40] Huagang Xie. LIDS Linux Intrusion Detection System <http://www.lids.org/> [Consulta: 6 julio 2002]

[41] Security Software Technologies, Inc. Antisniff <http://www.securitysoftwaretech.com/antisnif > [Consulta: 6 julio 2002]

[42] WU-FTPD Development Group. Wu-ftpd <http://www.wu-ftpd.org> [Consulta: 6 julio 2002]

[43] The ProFTPD Project. ProFTPD <http://www.proftpd.org> [Consulta: 6 julio 2002]

[44] The Sendmail Consortium. Sendmail <www.sendmail.org > [Consulta: 6 julio 2002]

[45] Pozicom Technologies Incorporated. EDIPro <http://www.pozicom.net/Sales/Catalog/EDI_P [Consulta: 6 julio 2002]

[46] GnuPGP <http://www.gnupg.org/ >[Consulta: 6 julio 2002]

[47] Trojnara, Michal et al. Stunnel <http://www.stunnel.org/ > [Consulta: 6 julio 2002]

[48] OpenBSD. OpenSSH <http://www.openssh.org> [Consulta: 6 julio 2002]

[49] OpenSSL <http://www.openssl.org> [Consulta: 6 julio 2002]

[51] Zope Corporation. ZOPE <http://www.zope.org/> [Consulta: 6 julio 2002]

[53] Sainio, Garth. Eyler, Pat. Yams: Yet Another Merchant System <http://yams.sourceforge.net/ [Consulta: 6 julio 2002]

[56] Bernstein, Dan. The Qmail Homepage <http://www.qmail.org > [Consulta: 6 julio 2002]

[57] Univerisity of Cambridge. Exim http://www.exim.org [Consulta: 6 julio 2002]

[58] Aegypten <http://www.gnupg.org/aegypten/> [Consulta: 6 julio 2002]

[60] W3C. Amaya <http://www.w3.org/Amaya/> [Consulta: 6 julio 2002]

[61] Leffler, Sam. Hylafax <http://www.hylafax.org/> [Consulta: 6 julio 2002]

[62] Knorr, Gerd. Video4Linux Links. <http://bytesex.org/xawtv/links.html> [Consulta: 6 julio 2002] [68] Gélinas, Jacques. Linuxconf <http://dns.solucorp.qc.ca/linuxconf/> [Consulta: 6 julio 2002]

[69] Cameron, Jaime. Webmin <http://www.webmin.com> [Consulta: 6 julio 2002]

[70] The OpenLDAP Foundation. Open LDAP <http://www.openldap.org> [Consulta: 6 julio 2002]

[73] OpenWall Project. John the Ripper password cracker <http://www.openwall.com/john/> [Consulta: 6 julio 2002]

[74]. Mirzazhanov, Adel I. APG (Automated Password Generator) <http://www.adel.nursat.kz/ap [Consulta: 6 julio 2002]

[75] Texas A&M University y otros. Tiger: TAMU Security Tools <http://savannah.gnu.org/projec <http://www.net.tamu.edu/network/tools/tiger.html> [Consulta: 19 agosto 2002]

[76] Farmer, Dan. COPS! <http://www.fish.com/cops/ > [Consulta: 6 julio 2002]

[77] Libes, Don. Mkpasswd <http://tcl.activestate.com/man/expect5.31/mkpasswd.1.html> [Consulta: 6 julio 2002]

[78] OpenWall Project. Passwdqc <http://www.openwall.com/passwdqc/> [Consulta: 6 julio 2002]

[79] Wu, Tom. The Stanford SRP Authentication Project <http://www-cs-students.stanford.edu/~tjw/srp/> [Consulta: 6 julio 2002]

[80] Zawinski, Jamie. Xscreensaver. <http://www.jwz.org/xscreensaver/> [Consulta: 6 julio 2002]

[81] Bagley, David A. Xlock <http://www.chez.com/vidalc/xlock/xlock.htm> [Consulta: 6 julio 2002]

[82] Yoshinori K. Okuji. Matzigkeit, Gordon et al. GNU GRUB <http://www.gnu.org/software/gru [Consulta: 6 julio 2002]

[83] McQuillan Jim, Colcernian Ron, Glutting Jim, Allie Billy, McInnis Jack, Lauffer Stephan, Baum Georg,. Collins Michael H, Balneaves Scott, Stanford Robbie, Williams Andrew, LTSP:Linux Terminal Server project <http://www.ltsp.org/index.php> [Consulta: 6 julio 2002]

[84] Karazniewicz Artur, Open PKI <http://sourceforge.net/projects/openpki/> [Consulta: 6 julio 2002]

[85] Massachusetts Institute of Technology. Kerberos:The Network Authentication Protocol <http://web.mit.edu/kerberos/www/> [Consulta: 6 julio 2002]

[86] Russell Rusty. Linux IP Firewalling Chains Ver 1.3.10 <http://netfilter.samba.org/ipchains/> [Consulta: 6 julio 2002]

[87] Kadlecsik Jozsef, Welte, Harald Morris, James. Boucher, Marc. Russell Rusty. Netfilter -Iptables <http://netfilter.samba.org/> [Consulta: 6 julio 2002]

[88] Eastep, Tom. Seawall: Seattle Firewall 4.1 <http://seawall.sourceforge.net/> [Consulta: 6 julio 2002]

[101] The FreeRADIUS Project. FreeRADIUS Server Project <http://www.freeradius.org > [Consulta: 6 julio 2002]

[103] Tourrilhes, Jean. Brattli, Dag. Heuser, Werner. Costin, Claudiu. Linux IrDA Project <http://irda.sourceforge.net/ > [Consulta: 6 julio 2002]

[104] Tourrilhes, Jean .Wireless Tools for Linux <http://www.hpl.hp.com/personal/Jean_Tourrilhe > [Consulta: 6 julio 2002]

[105] Kannel Foundation . Kannel: Open Source WAP and SMS gateway <http://www.kannel.3glab > [Consulta: 6 julio 2002]

[107] Lasser, Jon. Véale, Jay. et al. Bastille Linux <http://www.bastille-linux.org/ > [Consulta: 6 julio 2002]

[108] Powell, Brad. Titan <http://www.fish.com/titan/TITAN_documentation.html > [Consulta: 6 julio 2002]

[109] Tsai, Tim. Singh, Navjot. Libsafe: Protecting Critical Elements of Stacks <http://www.research.avayalabs.com/project/libsafe/> [Consulta: 6 julio 2002]

[110] Free Software Foundation, Inc. GDB Project Debugger <http://www.gnu.org/software/gdb/g > [Consulta: 6 julio 2002]

[111] Free Software Foundation, Inc. Checker <http://www.gnu.org/software/checker/checker.es.ht
> [Consulta: 6 julio 2002]
[112] LoopAes , <http://loop-aes.sourceforge.net/ > [Consulta: 6 julio 2002]
[113] Picaud, Benoît. Colombet, Laurence. IDX-PKI: Open Source implementation of a Public Key Infrastructure <http://idx-pki.idealx.org/ > [Consulta: 6 julio 2002]
[114] Pascal Molli et al. CVS Concurrent Versions System <http://www.loria.fr/~molli/cvs/doc/cvs_toc.html > [Consulta: 6 julio 2002].
[115] Miller Peter Aegis 4.5 Configuration Management System <http://aegis.sourceforge.net/> [Consulta: 6 julio 2002]
[125] Craig H. Rowland: Logcheck, <http://www.psionic.com/tools/>

7. Referencias Generales

Nota: Estas referencias pueden ser tomadas como base para crear la política que se ajusta a los puntos del código de buenas prácticas que puede cumplir nuestra empresa una vez evaluados los riesgos a los que se está expuesto. Puede

- SecurityFocus. Linux Security tools [en línea] <http://online.securityfocus.com/infocus/1423> [Consulta: 6 julio 2002]
- NSA. Security Enhanced Linux <http://www.nsa.gov/selinux/> [Consulta: 6 julio 2002]
- SecurityFocus. Linux Kernel Hardening <http://online.securityfocus.com/infocus/1539> [Consulta: 6 julio 2002]
- Stross, Charlie. Linux and Cryptography <http://www.antipope.org/charlie/linux/shopper/167 [Consulta: 6 julio 2002]
- Seifried, Kurt. Linux Administrator's Security Guide Ver: 1 Oct 2001. <http://www.seifried.org/ >[Consulta: 6 julio 2002]
- Gerhard Mourani and OpenDocs, LLC. and Madhusudan (Madhu "Maddy"). Securing and Optimizing Linux: RedHat Edition <http://www.tldp.org/LDP/solrhe/Securing-Optimizing-Linux-RH-Edition-v1.3/> [Consulta: 6 julio 2002]
- Naidu, Krishni. Auditing Linux <http://www.sans.org/SCORE/checklists/AuditingLinux.doc> [Consulta: 6 julio 2002]
- LinuxLinks.com Referencia a programas de backup <http://www.linuxlinks.com/Software/Back [Consulta: 6 julio 2002]
- Graham,Robert Antisniff FAQ Ver 0.3.3, 14 September, 2000 [en línea] <http://www.robertgraha faq.html >

- Reichard, Kevin. Implementing E-Commerce on Your Linux System Previews of TallyMan, Yams, and OpenMerchant [en línea] <http://www.linuxplanet.com/linuxplanet/rep [Consulta: 6 julio 2002]

- Hubert, Bert (Netherlabs BV). Maxwell, Gregory. Van Mook Remco. Oosterhout, Martijn Van. Schroeder, Paul B. Linux 2.4 \

Advanced Routing HOWTO \ <http://www.linuxdocs.org/HOWTOs/Adv-Routing-HOWTO-13.html> [Consulta: 6 julio 2002]

- Linuxdoc.org The linux documentation project <http://www.tldp.org/docs.html#howto.> [Consulta: 6 julio 2002]

- Friberg, Paul. Using a Cryptographic Hardware Token with Linux: the OpenSSL Project's New Engine [en línea] Ver: 20 Jun. 2001 <http://www.linuxjournal.com/article.php?sid 6 julio 2002]

- Spitzner, Lance. Armoring Linux. Ver: 19 Sep. 2000 <http://www.enteract.com/~lspitz/linux.html> [Consulta: 6 julio 2002]