5.2 Cuadros comparativos

Vistos los requerimientos técnicos de la ley y su resolución por parte de los sistemas de auditoría de las plataformas estudiadas, vamos a proceder a su análisis para poder sacar más adelante conclusiones útiles. Para ello, la forma más fácil de hacerse una idea del conjunto, es poner los resultados en una tabla comparativa en donde se ponderarán la capacidad de cubrir los apartados que componen los artículos técnicos del reglamento.

La ponderación se basará, únicamente, en la valoración de si el sistema es capaz de auditar el control que indica el reglamento en cada apartado y no en si el sistema dispone de las medidas de seguridad para cubrirlo. Si el sistema no dispone de las medidas de seguridad, está claro que no va a poder auditarlas, pero si las tiene, no está implícito que puedan ser auditadas, como veremos en el análisis.

La ponderación de cada apartado de cada artículo seguirá las reglas de la tabla siguiente:

Puntuación	Descripción
0	El SO no permite auditar por completo las medidas de seguridad de ese apartado.
1	El SO permite auditar completamente ese apartado.

Se ha escogido esta ponderación sin ningún tipo de gradación entre el 0 y el 1 ya que este es el criterio que toman los aditores. Es decir, o se cumple el apartado o no se cumple. Esto no quiere decir que haya apartados que en que el sistema operativo cumple parte del mismo y que la parte no cubierta puede serlo mediante *software* añadido. En caso de ser así, se indica el en punto de análisis de la página 104.

La tabla comparativa se encuentra en la siguiente página.

Nivel	Artículo	Apartado	Windows Server 2008	OS/400 V6R1	Red Hat Enterprise Linux 5
Todos	85	1	1	1	1
	87	1	0	1	0
		2	0	1	0
Básico	89	2	1	1	1
	90	1	0	1	0
	91	1	1	1	1
		2	1	1	1
		3	1	1	1
		4	1	1	1
	93	1	1	1	1
		2	1	1	1
		3	1	1	1
		4	1	1	1
	94	1	1	0	0
		2	0	1	0
Medio	98	1	1	1	1
	100	1	0	1	0
Alto	101	2	1	0	1
	103	1	1	1	1
		2	0	0	0
		3	1	1	1
	104	1	1	1	1

5.3 Análisis

El 100% de cobertura de los apartados técnicos del reglamento vigente de la ley de protección de datos, se consigue con 22 puntos y la distribución para las diferentes plataformas ha sido la siguiente:

Sistema Operativo	Puntos	Porcentaje sobre el total
Windows Server 2008	16	72,7%
OS/400 V6R1	19	86,3%
Red Hat Enterprise Linux 5	15	68,2%

Seguidamente se enumeran los artículos explicando el porqué de los resultados obtenidos por cada sistema.

Artículo 85

En este artículo que habla sobre la exigencia de que los requerimientos de seguridad sean aplicables tanto al acceso local como al acceso remoto, no supone problema alguno para que los sistemas estudiados lo puedan cumplir y permitan auditar que se cumple. Los tres sistemas están diseñados para que su función se desarrolle en un entorno de red donde los accesos son remotos y por tanto las medidas se seguridad son las mismas tanto, para una situación como para la otra.

Es por ello que los tres sistemas operativos obtienen la máxima puntuación.

Artículo 87

El correcto tratamiento de los ficheros temporales o copias de ficheros con datos personales, únicamente, está cubierto completamente por *OS/400* gracias a su capacidad de auditar ficheros de *spool* así como de ficheros en las bibliotecas temporales (*QTEMP*) que son eliminadas automáticamente después de la muerte de cada trabajo.

Los demás sistemas operativos cumplen parcialmente.

Artículo 89

Los tres sistemas no tienen problema alguno en auditar el cumplimiento, de que se esté informando a los usuarios que acceden al sistema. Realmente este requerimiento era muy básico y no debía presentar ningún problema.

Windows es el único que tiene una opción específica en sus políticas de seguridad, para el cumplimiento de un requerimiento de este tipo. Para los otros dos sistemas se utilizan funcionalidades que se usan para otros menesteres, pero que pueden servir para este.

La auditoría del cumplimiento de la obligación de informar, tampoco presenta mayores problemas.

Artículo 90

En este artículo pinchan los tres sistemas en mayor o menor medida. El artículo indica la necesidad de un registro de incidencias, y en la mayoría de los casos, esto se lleva a cabo de manera manual o mediante herramientas específicas para ello por parte del responsable

de seguridad. Pero no existe razón alguna para que los registros de auditoría, *Event Log* para Windows, *audit journal* para *OS/400* y *audit trail* para Linux, no permitan el añadir comentarías *adhoc* a los mensajes de auditoría. Esto enriquecería el histórico de auditoría y se cumpliría de manera nativa, por parte de los sistemas operativos, la necesidad de disponer de un registro de incidencias. El sistema que más se acerca a este concepto, es *OS/400* ya que su *audit journal* y sus *journal* de bases de datos, permiten que se añadan registros *adhoc* garantizando que lo que haya dentro no podrá ser alterado.

Artículo 91

El control de acceso a los datos es una de las tareas principales de cualquier subsistema de seguridad, y por tanto, no sorprende que los tres sistemas sean capaces de garantizar el control de acceso por las medidas de seguridad que implementan y por su capacidad de auditar que las reglas establecidas de acceso se están cumpliendo.

Artículo 93

Lo mismo pasa con el artículo 93. La identificación y autenticación son básicas en un sistema mínimamente seguro. Los tres sistemas son capaces de auditar, sin problemas, que se están cumpliendo los mecanismos de identificación y autenticación.

Artículo 94

Este artículo, que trata sobre las copias de respaldo y restauración, es bastante sorprendente a la hora de analizar cómo los sistemas auditan su cumplimiento. *Windows* es el que mejor se comporta, ya que tanto las copias como las restauraciones realizadas mediante sus herramientas nativas, dejan trazas de auditoría. El único punto débil que tiene, es que no es capaz de reconstruir un fichero de datos dañado en cualquier momento del tiempo, únicamente es capaz de restaurar el estado en que se encontrada en la última copia de seguridad.

El sistema *OS/400* no deja mensajes de auditoría cuando se realiza copias de seguridad, aunque si lo hace sobre un *log* histórico (*QHST*), pero no debe considerarse este *log* como de auditoría porque no tiene las garantías de seguridad que si tiene *QAUDJRN*. En cambio las restauraciones de objetos sí dejan trazas de auditoría. *OS/400* sí es capaz de restaurar un fichero de datos (fichero físico) a su estado original en cualquier momento, gracias a la funcionalidad de la *journalización* de bases de datos. Aquí OS/400 parte con ventaja al ser un sistema con un motor de base de datos integrado y se vale del registro de transacciones para el cumplimiento de regulaciones de seguridad.

Linux es el peor sistema, en cuanto a salvado y restaurado de copias de seguridad realizadas de manera nativa, más que nada porque no da esta funcionalidad. Es necesario indicar que existen muchísimas opciones no nativas para hacerlo, como son aplicaciones libres, o *scripts* propios, que tendrán sus propios *logs* o enviarán eventos a *syslog*, pero no dejan trazas en al *audit trail*.

Artículo 98

Todos los sistemas son capaces de limitar el número de intentos de acceso fallido al sistema y también de auditar el correcto funcionamiento del control.

Artículo 100

Este artículo está ligado al artículo 94 por el hecho de hablar sobre la recuperación de datos, pero también está relacionado con el 90 por ser el registro de incidencias. En este caso es *OS/400* el único que permite la auditoría de la recuperación, junto con la inserción

de mensajes *adhoc* en el registro de auditoría. *Windows* por un lado si registra recuperaciones pero no permite la inserción de mensajes *adhoc*, y *Linux* ya falla en lo principal, que es auditar la recuperación de datos.

Artículo 101

En la confidencialidad de los datos residentes en soportes que se distribuyen, *OS/400* muestra una importante debilidad, ya que no permite el cifrado de esos datos. Únicamente permite cifrar campos concretos en ficheros físicos pero es un argumento muy débil, ya que no se utiliza por temas de rendimiento. El cifrado de soportes se consigue con aplicaciones de terceros pero no nativamente.

En cambio, *Windows* y *Linux* cumplen perfectamente con esta funcionalidad requerida y la auditoría del cumplimiento es posible.

Artículo 103

El artículo sobre el registro de accesos, en el primer apartado, pide registrar cuándo, quién y sobre qué fichero de datos se ha intentado acceder y su resultado. El registro de accesos es la funcionalidad más primordial de todo subsistema de auditoría y por tanto, no debe extrañar que los tres sistemas operativos sean capaces de cumplirlo sin problemas.

El segundo apartado es uno de los más controvertidos, sino el que más, del Real Decreto ya que reclama una auditoría de los datos concretos a los que se ha accedido. Como ya se ha comentado con anterioridad este requerimiento es una de las pesadillas de los responsables de seguridad por la complejidad técnica que implica y por el impacto en el rendimiento de las máquinas y las aplicaciones que supone.

El sistema que mejor se adapta a este complicado requerimiento es *OS/400*, gracias otra vez a su *journal* de base de datos que registra todos los cambios a nivel de registro en las tablas de datos. La única limitación es que no registra los accesos de lectura (las operaciones *SELECT* de *SQL*), aunque esto es fácilmente solucionable con herramientas externas o desarrollos propios, el hecho de no ser nativo hace que tenga un cero en vez de todo el punto. Los demás sistemas operativos, únicamente, son capaces de registrar accesos a nivel del objeto (apartado uno del artículo) pero no a nivel de registro ni campo. Por tanto tienen una puntuación de cero.

Esta debilidad estructural de *Windows* y *Linux* respecto a la auditoría a nivel de registro puede llegar a solucionarse obligando a que todo fichero sensible sea una base de datos almacenada en un motor que tenga auditoría propia, como por ejemplo *SQLServer* u *Oracle*. Cumpliendo esta obligación y auditando a nivel de registro mediante el motor de base de datos, estos dos sistemas operativos podrían cubrir este importante apartado.

El tercer apartado, que requiere que la auditoría esté bajo control de personal autorizado, es cumplido por todos los sistemas, los cuales permiten auditar su cumplimiento sin problemas.

Artículo 104

Todos los sistemas estudiados permiten cifrar las comunicaciones entrantes y salientes mediante criptografía fuerte, y también permiten auditar que las políticas que definen las conexiones seguras se cumplen correctamente.

Capítulo 6
Planificación

6.1 Planificación inicial

- Definición del proyecto: 15 horas
- Investigación del contexto legislativo sobre protección de datos: 100 horas
- Instalación de las plataformas a analizar: 10 horas
- Búsqueda de información sobre los subsistemas de auditoría de las plataformas a analizar: 150 horas
- Configuración de los subsistemas de auditoría: 50 horas
- Estudio del cumplimiento del reglamento por parte de la auditoría de las plataformas analizadas y creación de la comparativa: 150 horas
- Investigación de *software* específico para el cumplimiento de la ley de protección de datos: 20 horas
- Instalación y pruebas del software especifico para el cumplimiento de la ley de protección de datos: 50 horas
- Realización del documento de informe del proyecto: 4 horas
- Realización de la memoria del proyecto: 45 horas
- Creación de la presentación de defensa del proyecto: 20 horas

Total previsto: 609 horas de trabajo

6.2 Planificación final

- Definición del proyecto: 15 horas
- Investigación del contexto legislativo sobre protección de datos:
    - Normativa estatal: 75 horas
    - Normativa catalana: 20 horas
    - Normativas de otros países (Francia, EUA): 15 horas
- Asistencia a dos seminarios sobre el nuevo reglamento LOPD: 8 horas
- Instalación de las plataformas a analizar:
    - Windows : 5 horas
    - OS/400: 10 horas
    - Linux: 5 horas

- Búsqueda de información sobre los subsistemas de auditoría de las plataformas a analizar:
    - Windows: 50 horas
    - OS/400: 50 horas
    - Linux: 35 horas
- Configuración de los subsistemas de auditoría:
    - Windows : 10 horas
    - OS/400: 15 horas
    - Linux: 15 horas
- Estudio del cumplimiento del reglamento por parte de la auditoría de las plataformas analizadas y creación de la comparativa: 160 horas
- Investigación de *software* específico para el cumplimiento de la ley de protección de datos: 25 horas
- Instalación y pruebas del software especifico para el cumplimiento de la ley de protección de datos: 40 horas
- Realización del documento de informe del proyecto: 4 horas
- Realización de la memoria del proyecto: 45 horas
- Creación de la presentación de defensa del proyecto: 20 horas
- Diseño de una demostración de auditoría en tiempo real para la defensa del proyecto: 15 horas

Total realizado: 637 horas de trabajo

La desviación entre el tiempo previsto y el tiempo realizado es de un incremento del número de horas en un 4,6%. Este incremento está dentro de los parámetros que se consideran aceptables para la desviación de proyecto de consultoría, que suele estar sobre el 10%, y se debe principalmente a la posibilidad que se me presentó de asistir a dos seminarios sobre el nuevo reglamento. El primero organizado por un conocido el bufete de abogados barcelonés, y el segundo por la *EAE* al que asistió la presidenta de *l'Agència Catalana de Protecció de Dades*, doctora Esther Mitjans i Perelló. Otro factor de desviación está en que he creído conveniente diseñar una configuración de un *software* de monitorización para enseñar durante la defensa del proyecto como auditar en tiempo real las plataformas estudiadas.

6.3 Costes del proyecto

Este trabajo bien podría haber sido un encargo como proyecto de consultoría de una empresa con la necesidad de conocer el grado de cumplimiento del nuevo reglamento por parte de sus plataformas. Su completa realización es de 637 horas de trabajo. Ciertas partes del proyecto como la instalación de software o la documentación pueden ser realizadas por un consultor *junior* y que el resto debería ser realizado por un consultor *senior*. La siguiente tabla muestra un desglose de costes:

Recursos	Número	Horas	Precio/Hora	Precio
Consultor *senior*	1	512	80 €/hora	40.960 €
Consultor *junior*	1	125	40 €/hora	5.000
TOTAL	**2**	**637**	**-**	**45.960 €**

Capítulo 7
Conclusiones

Este resultado del análisis nos indica que los tres sistemas operativos cumplen una parte importante de los requerimientos técnicos del nuevo reglamento de protección de datos, aunque ninguno de ellos lo cubre de manera completa. El mejor preparado es *OS/400 V6R1*, con un 86,3%. Los otros dos sistemas están cerca uno de otro, siendo el segundo mejor *Windows Server 2008* con un 72,7% y finalmente *Red Hat Linux Enterprise 5* con un 68,2%.

Puntos débiles

Existen ciertas similitudes en los puntos débiles de los sistemas estudiados.

El registro de incidencias no es algo que esté bien resuelto en los sistemas operativos estudiados. En los artículos 90 y 100 se requiere que exista un registro de incidencias para que se puedan insertar anotaciones de los responsables de seguridad sobre las incidencias ocurridas y su resolución, así como de las recuperaciones de datos. *Windows* y *Linux* tienen *logs* de auditoría, pero no están diseñados para que se puedan insertar anotaciones *adhoc*. Únicamente *OS/400* permite insertar anotaciones, aunque no de manera fácil. Para *Windows* y *Linux* es necesario recurrir a aplicaciones de terceras empresas o a simples documentos mantenidos manualmente. Como soluciones externas, existen los productos *online Pack LOPD* de la web derecho.com o también las aplicaciones de escritorio de la empresa *Gesdatos Software, S.L.* Ambos disponen de buenos módulos para el registro de incidencias.

Otro punto débil de los sistemas estudiados, es el cumplimiento del problemático y controvertido apartado dos del artículo 103, el que obliga a guardar la información que permita identificar los registros accedidos para un fichero con datos de nivel alto. Este registro de accesos de datos de nivel alto, es la auténtica pesadilla de los responsables de seguridad por el elevadísimo volumen de datos que puede llegar a generar en un sistema productivo. De manera nativa, el único sistema capaz de cumplir parcialmente es *OS/400*, aunque no para las lecturas. Los demás sistemas operativos, sin motor de base de datos embebido, no son capaces de ningún tipo de auditoría a nivel de registro y para ellos, se plantean dos alternativas: que la aplicación corporativa que utilice datos personales tenga su propia auditoría, o que los datos estén almacenados en un motor de base de datos que tenga auditoría a nivel de registro, como *SQLServer* u *Oracle*. *OS/400* puede complementar su auditoría a nivel de registro para registrar lecturas con el producto *DataMonitor for iSeries* de *Tango/04 Computing Group, S.L.*

La auditoría de las copias de seguridad es otro punto débil, en este caso compartido por *OS/400* y *Linux*. En *OS/400* los mandatos de salvado no dejan trazas de auditoría, y en

Linux, la gestión nativa de salvado y restaurado brilla por su ausencia. Para *Linux* existen multitud de aplicaciones externas que permiten realizar la gestión de las copias y de las restauraciones, como el *BrightStor ARCserve Backup for Linux* de *CA* o el gratuito y libre *Bacula*.

El cifrado de soportes es quizá la limitación más importante de *OS/400*. De hecho, *OS/400* no permite cifrar la información ni en soportes, ni en discos, ni a nivel de objeto de manera nativa. Para ello es necesario recurrir a productos de terceras partes, pero suponen un gasto extra a las empresas que quieren confidencialidad e integridad absoluta en su información almacenada. Otra opción, son los desarrollos propios usando las *APIs* criptográficas que el sistema operativo provee. Pero no existe una forma transparente de cifrado como el *EFS* de *Windows*, por poner un ejemplo.

Puntos fuertes

La gran ventaja de *OS/400* frente a sus rivales, es contar con un motor de bases de datos integrado con el que se gestionan los ficheros de datos. Esto le permite registrar todos los cambios efectuados a nivel de registro y de esta manera, cumplir parcialmente con el controvertido artículo 103. Únicamente le falla el hecho de no registrar los accesos de lectura (las *queries* de tipo *SELECT*), pero se entiende que eso no haya sido previsto por el fabricante ya que la *journalización* está diseñada para la reconstrucción de los datos o para el control de *commit* (*Commitment Control*) y no para la auditoría, con lo cual, el registro de las lecturas no es necesario. No estaría de más que *IBM* permitiera la opción de *journalizar* también las lecturas y que fuera una opción a escoger por el oficial de seguridad.

El cifrado de discos completamente transparente para el usuario de *Windows* mediante su tecnología *EFS*, es un punto a su favor muy importante porque permite proteger los ordenadores portátiles o los discos duros externos u otros soportes de cualquier otro tipo que contengan datos importantes y de esta manera, facilitar su distribución y almacenaje seguro. La auditoría del uso de *EFS* es muy completa. *Linux* aporta la misma funcionalidad mediante *md_crypt*, aunque auditar que está funcionando correctamente es bastante complejo y no es del todo completa.

Linux tiene muchos puntos fuertes, pero en ningún punto de este trabajo ha podido superar a sus competidores de manera clara. Su baza más importante, que es la robustez, la seguridad intrínseca y la gran comunidad de programadores que se encargan de mantener los *bugs* a ralla, no lo hacen más auditable y puede ser un criterio de descarte como plataforma escogida para mucho gestores de las TIC.

Resumen y valoraciones finales

Vistos los resultados, *OS/400* es sin duda el sistema operativo más enfocado a la auditoría. Esto es así, porque desde siempre ha sido una plataforma presente en sectores empresariales con importantes requerimientos para el cumplimiento de leyes y regulaciones, lo que los americanos le llaman *"compliance"*. Su sistema de auditoría provee de casi todo lo necesario para cubrir las normativas financieras como la *SOX*, sobre salud como la *HIPAA* o normas de la industria de las tarjetas de crédito como *PCI*.

La configuración de la auditoría de *OS/400* es algo compleja y poco intuitiva, pero no es necesaria la correlación de eventos para una única situación de seguridad, a parte que, las descripciones de los mensajes de auditoría son muy claros y muy completos, con toda la información necesaria para facilitar el trabajo al auditor.

La auditoría de *Windows* es bastante potente y de muy fácil configuración. La posibilidad de forzar políticas de auditoría a todos las máquinas de un dominio mediante el *Active Directory*

es una bendición para los administradores de sistemas. Los puntos débiles que presenta son pequeños, y menos el de auditoría de acceso a nivel de registro, que es estructural, todos los demás pueden ser cubiertos fácilmente en futuras versiones. Un punto de mejora podría ser el hecho de que *Windows* genera muchos eventos para una única situación de seguridad y esto hace, que no sea trivial el análisis de lo ocurrido a nivel de auditoría ya que es necesario correlacionar varios eventos para averiguar exactamente lo que pasó. Una redefinición de los eventos y de la manera en que se registran, sería conveniente para facilitar la tarea del auditor.

Existe la opinión que *Linux* es un sistema bastante seguro, quizá más que *Windows* y es muy posible que sea verdad, lo que está claro es que no es más auditable. La gestión de la auditoría de *Linux* es terrible por engorrosa. Por ejemplo, hay que añadir manualmente todos y cada uno de los ficheros que se quieren auditar en un fichero de configuración; o que la creación de reglas es a nivel de llamadas al sistema, con lo cual es complejo ver qué situaciones se están realmente auditando, a parte, de ser poco mantenible. Los mensajes de auditoría son tremendamente crípticos y muchas veces se echa a faltar algo más de información del contexto del evento. Pero no todo es malo, porque por ejemplo, el comando *aureport* de generación de estadísticas de auditoría es una funcionalidad realmente útil y no tiene contrapartida en los otros sistemas.

Linux ha evolucionado mucho y seguirá haciéndolo gracias a su dinamismo por el hecho de ser de código abierto. Antes de la versión 2.6 del *kernel*, no existía un sistema de auditoría como tal. Ahora existe, aunque con puntos débiles, pero seguro que las futuras revisiones del núcleo añadirán mejoras tanto en nuevas capacidades de auditoría como en facilidad de gestión de la misma con interfaces más amigables.

Capítulo 8
Bibliografía

8.1 Bibliografía impresa

La Guía del AS/400

- Autor: Manuel Rincón
- Editorial: IDG Comunications, S.A.

OS/400 Primer

- Autores: Ernie Malaga, Doug Pence, Ron Hawkins
- Editorial: MC Press

Implementing AS/400 Security

- Autores: Carol Woodbury & Wayne Madden
- Editorial: News/400 Books

System iSecurity Security reference Version 6 Release 1

- Autores: Varios
- Editorial: IBM Corporation

Guía de seguridad de Microsoft Windows Server 2003

- Autores: Kurt Dillard, José Maldonado, Brad Warrender
- Editorial: Microsoft Technet

La protección de datos personales. Soluciones en entornos Microsoft

- Autores: Gonzalo Gallo, Iñigo Coello de Portugal, Fernando Larrondo, Héctor Sánchez
- Editorial: Microsoft Press

Red Hat Enterprise Linux 5 Security Guide

- Autores: Varios
- Editorial: Red Hat, Inc.

The Linux Audit Framework

- Autores: Varios
- Editorial: Red Hat, Inc.

8.2 Recursos en la red

Enlaces sobre legislación

Boletín oficial del estado: www.boe.es

Agencia española de protección de datos: www.agpd.es

Agencia catalana de protección de datos: www.apdcat.net

Parlamento europeo: www.europarl.europa.eu

Información sobre leyes norteamericanas: en.wikipedia.org

Enlaces sobre seguridad y auditoría

Cambios en la auditoria de Windows 2008 respecto a 2003:

http://blogs.technet.com/askds/archive/2007/10/19/introducing-auditing-changes-in-windows-2008.aspx

Auditoría de Windows 2008:

http://blogs.dirteam.com/blogs/jorge/archive/2008/04/29/auditing-in-windows-server-2008.aspx

Listado de Event IDs de seguridad de Windows 2008:

http://support.microsoft.com/kb/947226

Referencia en línea de OS/400

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp

Manual en línea de los comandos Linux

http://linuxcommand.org/

Ejemplos de auditoría de ficheros en Linux

http://www.cyberciti.biz/tips/linux-audit-files-to-see-who-made-changes-to-a-file.html

Enlaces a software específico de auditoría LOPD

http://www.tango04.com/solutions/security/

http://www.gesdatos.com/

http://www.ingeniusteam.com/Webcpi/index.aspx?pag=lopd4.htm

http://www.iniziaslopd.com/

http://www.susdatos.es/index.php?opcion=pack

Capítulo 9
Anexos

9.1 Software de auditoría de terceras partes

DataMonitor for iSeries

- Fabricante: Tango/04 Computing Group, S.L.
- Plataforma: OS/400
- Descripción: Permite la generación de múltiples reportes de auditoría a nivel de registro de ficheros físicos para el cumplimiento de LOPD, SOX, etc. Añade la posibilidad de auditar las lecturas a nivel de registro.

Visual Security Suite

- Fabricante: Tango/04 Computing Group, S.L.
- Plataforma: OS/400
- Descripción: Conjunto de agentes que recolectan información tanto del *journal* de seguridad como de otras fuentes, como el *log* histórico y permiten tener visibilidad sobre los trabajos, colas de mensajes, etc. Permite monitorizar fácilmente los trabajos de copia, los usuarios inactivos, las sentencias SQL tanto interactivas como ejecutadas por programas.

DataMonitor for SQLServer

- Fabricante: Tango/04 Computing Group, S.L.
- Plataforma: Windows
- Descripción: Permite la auditoría a nivel de registro en bases de datos SQLServer. La única operación que no registra son las lecturas.

Snare for Linux

- Fabricante: InterSect Alliance Pty Ltd.
- Plataforma: Linux
- Descripción: Snare es toda una familia de agentes multiplataforma. Destaca su módulo para Linux. A parte de leer del *audit trail* consulta otros *logs* del sistema para crear reportes muy completos. Está especializado en *"compliance"* de regulaciones norteamericanas como SOX o HIPAA, pero buena parte puede utilizarse para la LOPD.

gENRED

- Fabricante: CPI, S,A.
- Plataforma: N/A
- Descripción: Este es un software que permite gestionar toda la parte más burocrática de la LOPD, formularios, documentación, etc. A partir de sencillas pantallas permite crear automáticamente el documento de seguridad. También permite mantener un registro de incidencias bastante completo.

Gesdatos

- Fabricante: Gesdatos Software, S.L.
- Plataforma: N/A
- Descripción: Software parecido al de gENRED. Muy enfocado a gestión a la gestión LOPD para multiorganizaciones. Tiene un paquete especial para consultores en LOPD.

9.2 Tablas

9.2.1 "Entry types" de OS/400 V6R1

Entry Type	Descripción
AD	Auditing changes
AF	Authority failure
AP	Obtaining adopted authority
AU	Attribute changes
CA	Authority change
CD	Command string audit
CO	Create object
CP	User profile changed, created, or restored
CQ	Change of *CRQD object
CU	Cluster Operations
CV	Connection verification
CY	Cryptographic Configuration
DI	Directory Server
DO	Delete object

DS	DST security password reset
EV	System environment variables
GR	Generic record
GS	Socket description was given to another job
IM	Intrusion monitor IP Interprocess Communication
IR	IP Rules Actions
IS	Internet security management
JD	Change to user parameter of a job description
JS	Actions that affect jobs
KF	Key ring file
LD *	Link, unlink, or look up directory entry
ML	Office services mail actions
NA	Network attribute changed
ND	APPN directory search filter violation
NE	APPN end point filter violation
OM	Object move or rename
OR	Object restore
OW	Object ownership changed
O1	(Optical Access) Single File or Directory
O2	(Optical Access) Dual File or Directory
O3	(Optical Access) Volume
PA	Program changed to adopt authority
PG	Change of an object's primary group
PO	Printed output
PS	Profile swap
PW	Invalid password

RA	Authority change during restore
RJ	Restoring job description with user profile specified
RO	Change of object owner during restore
RP	Restoring adopted authority program
RQ	Restoring a *CRQD object
RU	Restoring user profile authority
RZ	Changing a primary group during restore
SD	Changes to system distribution directory
SE	Subsystem routing entry changed
SF	Actions to spooled files
SG	Asynchronous Signals
SK	Secure sockets connections
SM	Systems management changes
SO	Server security user information actions
ST	Use of service tools
SV	System value changed
VA	Changing an access control list
VC	Starting or ending a connection
VF *	Closing server files
VL	Account limit exceeded
VN	Logging on and off the network
VO	Validation list actions
VP	Network password error
VR *	Network resource access
VS	Starting or ending a server session
VU	Changing a network profile

VV	Changing service status
X0	Network Authentication
X1	Identify Token XD Directory server extension
XD	Directory server extension
YC *	DLO object accessed (change)
YR *	DLO object accessed (read)
ZC *	Object accessed (change)
ZR *	Object accessed (read)

* - *"Entry types"* que no se habilitan por los valores que tome QAUDLVL sino que se activan todas en bloque en caso de que exista el valor *OBJAUD en QAUDCTL.