CUORE

Número HS

Marzo 2011

Precio: 6,50 €

Una publicación de la Comunidad de Usuarios de Oracle España

www.cuore.es

El futuro de Cloud Computing a debate en el XX CONGRESO DE USUARIOS DE ORACLE Madrid, 16 y 17 de marzo

Entrevistas:

Maximo Aborruza,
Vicepresidente de la Comunidad de Usuarios

Rafael Ruiz,
vocal del grupo JD Edwards en CUORE

José Peláez,
Director de Soluciones de Oracle Ibérica

VIVAT ACADEMIA

Vivat Academia

revista de comunicación

Vicedecana de las revistas electrónicas universitarias españolas
www.ucm.es/info/vivataca

Editado por:
-El Departamento CAP II Facultad de CC.II. U. Complutense de Madrid (España)
-Decanato de la Fac. de Educación y Humanidades. U. de la Frontera (Chile)
-Concilium, Grupo de investigación oficial de la Universidad Complutense de Madrid
-SEECI, Sociedad Española de Estudios de la Comunicación Iberoamericana

Despacho 419. Fac. de CC.II. Avenida Complutense s/n. 28040 Madrid (España)
Tlf: (00 34) 91 394 21 67
Fax: (00 34) 91 394 22 80
Contacto: vivatacademia@ccinf.ucm.es

ISSN: 1575-2844

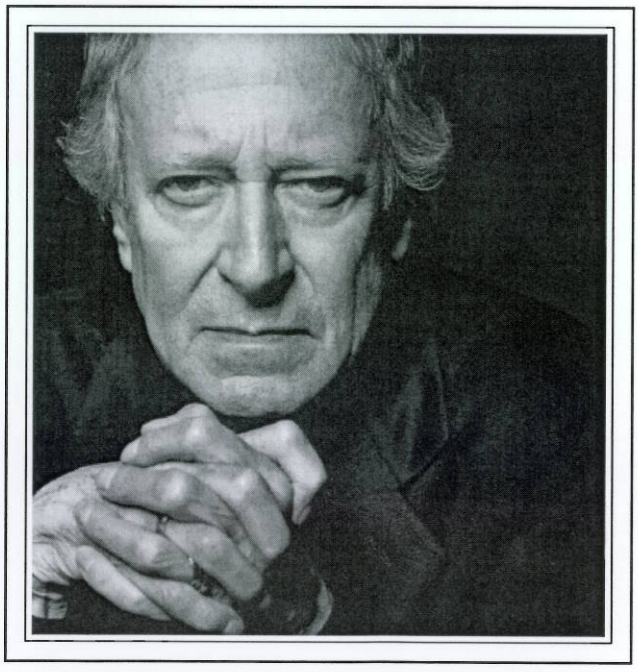
La Revista Vivat Academia publica sus nuevos números los meses de Marzo, Junio, Septiembre y Diciembre

Nº 114 -Marzo 2011- Año XIII

Google Buscar en sitio
Internet Vivat Academia

Puede encontrarnos en

latindex Catálogo y Directorio | IN~RECS
DD | uni>ersia
REBIUN | DICE
Dialnet
Google Académico BETA | e-revist@s
EBSCO HOST | CSIC ISOC



El 30 de Enero de 2011 murió el genio de las bandas sonoras, John Barry. "Bailando con lob "Memorias de África" o el tema de James Bond son algunos de los éxitos de su carrera en la consiguió 5 Oscars.

Descanse en paz.

VIVAT ACADEMIA

Nº28 (Parte 1) - MARZO 2011

Midiendo la Seguridad de los SGBD: Oracle y SQL Server

Luis Enrique Sánchez[1,2], Antonio Santos-Olmo1, Eduardo Fernández-Medina[2]

[1] Departamento I+D+i, Sicaman Nuevas Tecnologias
Juan José Rodrigo 4, 13700 Tomelloso

[2] Grupo de Investigación GSyA, U. Castilla-La Mancha
Paseo de la Universidad 4, 13071 Ciudad Real

[1] {Lesanchez, Asolmo}@sicaman-nt.com

[2] Eduardo.FdezMedina@uclm.es

RESUMEN

La sociedad de la información cada vez depende más de los Sistemas de Gestión de la Seguridad de la Información (SGSI), y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES. Sin embargo, este tipo de compañías requiere de SGSIs adaptados a sus especiales características, y que estén optimizados desde el punto de vista de los recursos necesarios para implantarlos y mantenerlos. Dentro de los SGSIs este artículo se ha centrado en el desarrollo de un proceso que permita medir los niveles de seguridad de aplicaciones críticas instaladas en los sistemas, en concreto los Sistemas Operativos y los Sistemas de Gestión de Bases de Datos. Este proceso está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.

1. INTRODUCCIÓN

Para las empresas, es muy importante implantar controles de seguridad que les permita conocer y controlar los riesgos a los que pueden están sometidas [1, 2]. Pero la implantación de estos controles no es suficiente, siendo necesarios sistemas que gestionen la seguridad a lo largo del tiempo, de modo que les permita reaccionar ágilmente ante nuevos riesgos, vulnerabilidades, amenazas, etc. [3]. Sin embargo, es frecuente que las empresas no tengan sistemas de gestión de seguridad, o que si los tienen, éstos estén elaborados sin unas guías adecuadas, sin documentación y con recursos insuficientes [4]. Además, la mayor parte de las herramientas de seguridad disponibles en el mercado ayudan a solucionar parte de los problemas de seguridad, pero son pocas las que abordan el problema de la gestión de la seguridad una manera global e integrada. De hecho, la enorme diversidad de estas herramientas y su falta de integración suponen un enorme coste en recursos para poderlas gestionar.

Por lo tanto, a pesar de que la realidad ha demostrado que para que las empresas puedan utilizar las tecnologías de la información y las comunicaciones con garantías es necesario disponer de guías, métricas y herramientas que les permitan conocer en cada momento su nivel de seguridad y las vulnerabilidades que aún no han sido cubiertas [5], el nivel de implantación con éxito de estos sistemas, realmente es muy bajo. Este problema se acentúa especialmente en el caso de las pequeñas y medianas empresas, que cuentan con la limitación adicional de no tener recursos humanos y económicos suficientes para realizar una adecuada gestión [4].

De acuerdo a investigaciones recientes [6], el éxito de los SGSI, depende principalmente de los siguientes factores: i) enfocar la seguridad hacia el negocio; ii) implementar la seguridad en consonancia con la cultura de la empresa; iii) conseguir el apoyo indiscutible, visible y comprometido de la dirección de la empresa; iv) conseguir entender bien los requisitos de seguridad, de la evaluación y gestión de los riesgos; v) concienciar tanto a directivos como a empleados de la necesidad de la seguridad; vi) ofrecer formación y guías sobre políticas y normas a toda la organización; vii) definir un sistema de medición para evaluar el rendimiento de la gestión de la seguridad y sugerir mejoras. Para el caso de las PYMEs, estos factores son importantes, pero además, el SGSI debe estar optimizado en cuanto a recursos necesarios, y también debe tener un alcance suficiente, para no descuidar la seguridad, pero no excesivo, para controlar su coste. Por ese motivo, es muy importante poder contar con metodologías para la gestión de la seguridad de la información que estén especialmente diseñados para este tipo de empresas, y que además permitan reutilizar el conocimiento, de modo que su implantación sea más rápida, más certera y más económica.

Por otro lado, el término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar vulnerabilidades. El concepto de auditoría es mucho más que esto. Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una empresa o una sección de la misma. La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos. En este documento nos centraremos en el estudio de una de la ramas de la Auditoría que más relevancia está tomando en la actualidad, las "Auditorías Informáticas".

Los principales objetivos que constituyen a la auditoría informática son el control de la función informática, el análisis de la eficiencia de los Sistemas de Información que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

La Auditoría Informática se hace más necesaria debido a la importancia de gestionar adecuadamente y controlar los Sistemas de Información que se puede deducir de varios aspectos. He aquí algunos:

- Los ordenadores y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia. En este caso interviene la Auditoría Informática de Seguridad.
- Los sistemas creados para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. El mantener una constante disponibilidad de la información del sistema, así como asegurar la calidad y corrección de la misma se convierte en un aspecto básico para el buen funcionamiento de una empresa.
- Un Sistema de Información mal diseñado puede convertirse en una herramienta peligrosa para la empresa: las maquinas obedecen ciegamente a las órdenes recibidas, con lo que la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados.

El problema al que se enfrenta el usuario en este tipo de sistema es la inseguridad creada. Preguntas del tipo: "¿están mis datos seguros?", "¿puedo perderlos?", "¿cómo puedo tener mayores garantías?" quedan sin respuesta.

De estas dudas, proviene la gran importancia que las auditorías informáticas han tomado en los últimos años, ya que son el mecanismo de determinar si este tipo de sistemas son o no seguros y de esa forma poder ofrecer unas mínimas garantías de seguridad a los propietarios de los datos.

El artículo continúa en la Sección 2, describiendo brevemente los objetivos que se han perseguido a lo largo de la investigación. En la Sección 3 se describe el proceso de medición utilizado. En la Sección 4 se analizan los objetivos de control elaborados para la fase actual de la investigación. En la Sección 5, se presenta la herramienta que da soporte al proceso definido y se muestran algunos de los resultados obtenidos. Finalmente, en la Sección 6 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

2. OBJETIVOS PERSEGUIDOS CON LA INVESTIGACIÓN

A partir de esta visión de la situación actual del mercado y de las necesidades de la empresas, se ha centrado el objetivo de esta investigación, en elaborar un proceso que permita medir de una forma sencilla, pero eficiente, el nivel de seguridad de aplicaciones que podemos considerar críticas para el correcto funcionamiento del Sistema de Información de una compañía., así como una herramienta que de soporte a este proceso y ofrezca la posibilidad de automatizar parte de las pruebas a efectuar en el sistema y obtener un informe final con el estado de securización de sus principales aplicaciones de trabajo. Este proceso permitirá obtener una garantía del riesgo que se asume con el Sistema Informático de una empresa, con un menor coste tanto en tiempo, como económico, lo que la hace de gran utilidad para las PYMES.

Los ámbitos en los que se ha centrado el análisis de los objetivos de control iniciales del procesos son:

- Sistema operativo: Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquéllas.
- Sistemas de Gestión de Base de Datos: El diseño de las Bases de Datos se ha convertido en una actividad muy compleja y sofisticada. La auditoría analizará los Sistemas de salvaguarda existentes, revisará la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

Por lo tanto, podemos definir que el principal objetivo de la investigación ha sido crear un proceso que permita definir una serie de aspectos medibles y valorables sobre aplicaciones críticas y una herramienta que lo soporte, la cual permita ofrecer una valoración objetiva y un informe

del riesgo actual de un sistema de almacenamiento de datos. El alcance de la fase actual de la investigación, se ha limitado a: a) Desarrollar todos los objetivos de control a nivel de Sistema Operativo y SGBD; b) Desarrollar una herramienta que de soporte al proceso y permita realizar la auditorias que contendrá todos los objetivos de control; c) Analizar qué objetivos de control pueden ser automatizados en el SGBD; y d) Su validación en los entornos de desarrollo y producción de la compañía Sicaman.

Para alcanzar el objetivo propuesto en la investigación, se han seguido tres fases claramente diferenciadas:

- Durante la 1ª de las fases se ha analizado como definir un sistema sencillo que nos permita valorar el nivel de seguridad actual de las aplicaciones críticas.
- Durante la 2ª fase se han extraído de las herramientas seleccionadas para la investigación, cuáles serían los principales factores a valorar para definir su nivel de seguridad. Se ha procedido a realizar un estudio en profundidad del S.O. Windows y de los dos SGBD más utilizados en Oracle y SQL Server, definiendo los objetivos de control que permitan realizar posteriores auditorías, así como el sistema de valoración que se utilizará para la securización del entorno.
- Durante la 3ª de las fases se ha creado una aplicación que permitirá servir de soporte a la realización de las Auditorías sobre el proceso definido en la fase 1ª. Como resultado se ofrecerá una valoración del grado de securización de los sistemas analizados según su configuración actual. También se obtendrán unas recomendaciones asociadas a las acciones a acometer para aumentar el nivel de securización. Dicha aplicación estará formada por cuatro partes: a) Entrada de parámetros para el análisis; b) Rellenar la parte manual del checklist; c) Escaneo de la parte automática del checklist; y d) Emisión del informe.
- Por último, en la 4ª de las fases, se aplicará el proceso y la herramienta que lo soporta sobre diversos sistemas que funcionan en la compañía Sicaman. Con este proceso se obtendrá un conjunto de resultados de las auditorías que permitirán determinar el nivel de securización actual de los sistemas de esta empresa, así como recomendaciones sobre cómo mejorarlo.

3. DESARROLLO DEL PROCESO DE MEDICIÓN

Para el desarrollo de esta fase se realizó una selección previa de aquellas herramientas y aplicaciones que ante un fallo de seguridad pudieran tener un mayor impacto en los servicios informáticos de una compañía. Los resultados de este estudio demuestran que el mayor riesgo asumido por una empresa es la pérdida o filtración no deseada de sus datos.

En base a los resultados de este análisis se llegó a la conclusión de que las aplicaciones críticas en cualquier sistema informático, que funcione bajo una plataforma Microsoft, son el S.O. y los sistemas de soporte a datos, por lo que se seleccionaron para el desarrollo del proyecto las siguientes aplicaciones: Sistemas Operativos Windows y Sistemas de Gestión de Bases de Datos Oracle y SQL Server.

El siguiente paso de esta fase fue determinar para cada una de esas aplicaciones cuáles eran sus objetivos de control, así como determinar unas pruebas y niveles que permitieran evaluar el nivel de riesgo actual del sistema.

Para desarrollar dichos objetivos de control se contó con la documentación técnica sobre seguridad ofrecida por las compañías propietarias de las aplicaciones, así como con la experiencia personal del equipo de desarrollo.

En base a este conocimiento, se seleccionaron para cada aplicación aquellos puntos que suponían mayor riesgo. Posteriormente cada uno de estos puntos se discretizó para poder cuantificarlo.

El mecanismo de cuantificación o valoración de los objetivos de control está basado tan solo en el conocimiento de las aplicaciones ofrecidos por los expertos, lo cual implica que pueden sufrir variaciones en versiones posteriores de la aplicación.

La estructura que se ha seguido para definir los objetivos de control ha sido:

- **Id:** Código único que permite identificar el objetivo de control y la aplicación a la que pertenece.
- **Nivel:** En el entorno global, a qué nivel afecta el objetivo de control.
- **Pregunta:** Objetivo de control perseguido.
- **Responsabilidad:** Quién es el responsable de aplicar dicho objetivo de control
- **Instante:** Determina en qué instante debería haberse testeado el objetivo de control. Permite segregar los objetivos de control en subfamilias para estudios estadísticos posteriores.
- **Acción:** Determina a qué zona corresponde el objetivo de control dentro del entorno de la aplicación. Permite segregar los objetivos de control en subfamilias para estudios estadísticos posteriores.
- **Configuración correcta:** Cómo debería estar el objetivo de control para considerase seguro.
- **Valoración:** Mecanismo de cuantificar el nivel de securización del objetivo de control.

Como conclusión a las auditorías, se obtendrá un nivel de securización de la aplicación, que será calculado como:

NR = (([PTVE]*100)/[PTVP])
NS = 100 – NR

- **NR:** Nivel de riesgo.
- **NS:** Nivel de securización.
- **PTVE:** Puntuación total de las vulnerabilidades encontradas.
- **PTVP:** Puntuación total de las vulnerabilidades posibles.

Tabla 1. Modelo conceptual de datos del SIW

Según el valor obtenido tendremos el riesgo asociado, discretizado en la siguiente tabla:

Riesgo	Intervalo (según el nivel de securización)	Descripción
Sin Riesgo	90% - 100%	No se han detectado fallos graves.
Riesgo potencial	60% - 90%	Se han detectado fallos de nivel medio.
Alto riesgo	0% - 60%	Se han detectado uno o varios fallos de nivel alto.

Tabla 2. Modelo conceptual de datos del SIW

A continuación, se muestran de forma detallada todos los objetivos de control en los que se basarán las posteriores auditorías.

4. ISO/IEC 1504 Y EL MODELO CMMI

En esta fase de la investigación, se han analizado en detalle un conjunto de aplicaciones críticas, con el objetivo de extraer el conjunto de objetivos de control para cada una de las aplicaciones que han formado parte de la investigación. En la Tabla 3, se puede ver un ejemplo de control definido para esta aplicación. Las aplicaciones analizadas han sido:

- **Windows Server:** Se ha extraído un conjunto de 25 controles a valorar. El total de puntos que definirá el nivel de securización de la aplicación varia de 0 (máximo nivel de securización) a 37 (mínimo nivel de securización). Los aspectos a valorar se encuentras divididos en 5 tipologías:
  - Nivel de acceso: Incluye 8 aspectos valorables que afectan a los accesos del sistema.
  - Nivel de servicio: Incluye 8 aspectos que afectan a

los servicios del sistema, y a los usuarios con acceso a ellos.
- Nivel de aplicaciones: Incluye 3 aspectos que afectan a la seguridad en aplicaciones instaladas en el sistema.
- Nivel de gestión: Incluye 8 aspectos que afectan a la gestión y administración del sistema.
- Nivel de red: Incluye 2 aspectos que afectan a la configuración de red, así como vulnerabilidades sensibles de ser explotadas desde el exterior.

Id: [W2K.4.6]
Pregunta: ¿Existe copia de seguridad de los contenidos del Registro?
Nivel: Gestión.
Responsabilidad: Administrador
Instante: Operativa.
Acción: Registro
Configuración correcta: Mantener una copia de seguridad actualizada del Registro.
Valoración:
- ***Inseguro***: No existe una copia del registro, o ésta no se realiza periódicamente.
- ***Seguro***: Existe una copia de seguridad actualizada del registro, y esta se realiza periódicamente en periodos definidos.

Tabla 3. Control Manual para Windows Server.

- **SQL Server**: Se ha extraído un conjunto de 37 controles sobre los que valorar el nivel de cobertura de seguridad, de los cuales 26 pueden ser automatizados para reducir costes y 13 requieren actualmente de un análisis manual. El total de puntos que definirá el nivel de securización de la aplicación varia de 0 (máximo nivel de securización) a 53 (mínimo nivel de securización). Los aspectos a valorar se encuentras divididos en 4 tipologías:
  - Nivel general: Incluye 4 aspectos valorables que afectan directamente al entorno de la máquina, sobre la que se encuentra implantado el SGBD.
  - Nivel servidor: Incluye 3 aspectos valorables que afectan directamente a la configuración del servidor, sobre el que se encuentra implantado el SGBD.
  - Nivel SGBD: Incluye 26 aspectos valorables que afectan directamente al Sistema de Gestión de Base de Datos.
  - Nivel BD: Incluye 4 aspectos valorables que afectan directamente a las Bases de Datos.

- **Oracle:** Se ha extraído un conjunto de 26 controles sobre los que valorar el nivel de cobertura de seguridad. El total de puntos que definirá el nivel de securización de la aplicación varia de 0 (máximo nivel de securización) a 44 (mínimo nivel de securización). Los aspectos a valorar se encuentras divididos en 4 tipologías:
  - Nivel general: Incluye 6 aspectos valorables que afectan directamente al entorno de la máquina, sobre la que se encuentra implantado el SGBD.
  - Nivel servidor: Incluye 5 aspectos valorables que afectan directamente a la configuración del servidor, sobre el que se encuentra implantado el SGBD.
  - Nivel SGBD: Incluye 10 aspectos valorables que afectan directamente al Sistema de Gestión de Base de Datos.
  - Nivel BD: Incluye 5 aspectos valorables que afectan directamente a las Bases de Datos.

En el siguiente apartado se verán en detalle los controles definidos para valorar la seguridad de las aplicaciones de BD seleccionadas. Por motivos de espacio, se han dejado fuera del artículo los objetivos de control definidos para el Sistema Operativo.

4.1 OBJETIVOS DE CONTROL DEFINIDOS PARA SQL SERVER

Es este apartado se analizan los diferentes objetivos de control definidos para poder medir el nivel de seguridad sobre un SGBD SQL Server.

- **Nivel General:** Contiene los aspectos que afectan directamente al entorno de la máquina, sobre la que se encuentra implantado el SGBD. Estará formado por 4 aspectos valorables:
  - SQL1.1: El aspecto a valorar será "¿El servidor de BD es accesible físicamente por personal no autorizado?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Configuración del entorno previo a la Instalación" y podemos englobarla dentro de una acción de "Seguridad física". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Establecer un sistema de control de acceso a las instalaciones y al servidor; ii) Nombrar un responsable del servidor, que se ocupe de controlar los accesos; y iii) Realizar auditorías periódicas para verificar que se cumplen las políticas y procedimientos establecidos. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: El servidor de BD es accesible físicamente por personal no autorizado; y ii) Seguro: El servidor de BD no es accesible físicamente por personal no autorizado. Este objetivo de control se valorara de forma "automática", y la prueba solicitada estará formada por los siguientes pasos: i) Solicitar archivos de control de acceso a las instalaciones y al servidor. Políticas y procedimientos; ii) En caso de existir el archivo de control de acceso, verificar si este actualizado y iii) Si el archivo existe y esta actualizado el objetivo de control se considera cubierto y por tanto será seguro.
  - SQL1.2: El aspecto a valorar será ¿El almacenamiento de la copias de seguridad se realiza en una ubicación externa y segura?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Modelo y copias de seguridad". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Utilizar de forma adecuada el modelo de seguridad de SQL Server; y ii) Realice copias de seguridad de todos los datos con regularidad y almacene las copias en una ubicación externa segura. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: El almacenamiento de la copias de seguridad no se realiza en una ubicación externa y segura; y ii) Seguro: El almacenamiento de la copias de seguridad se realiza en una ubicación externa y segura. Este objetivo de control se valorara de forma "manual", y la prueba solicitada estará formada por los siguientes pasos: i) Verificar el lugar de almacenamiento de las copias de seguridad; y ii) En caso de no existir copias de seguridad, no estar adecuadamente catalogadas, o almacenarse en unas instalaciones internas, se considerara que el objetivo de control no está cubierto.
  - SQL1.3: El aspecto a valorar será "¿Se realizan periódicamente restauraciones de las copias de seguridad?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Modelo y copias de seguridad". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Utilizar de forma adecuada el modelo de seguridad de SQL Server; y ii) En caso de error del SGBD, verificar que la última copia de seguridad se realizó correctamente. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: No se realizan periódicamente restauraciones de las copias de seguridad; y ii) Seguro: Se realizan periódicamente restauraciones de las copias de seguridad. Este objetivo de control se valorara de forma "manual", y la prueba solicitada estará formada por los siguientes pasos: i) Verificar si existe algún documento de seguridad que contenga las restauraciones de las copias de seguridad, o preguntar al administrador; ii) En caso de no existir el documento o no estar actualizado, se considerara que el objetivo de control no está cubierto; y iii) En caso de producirse un error del SGBD, verificar que la

última copia de seguridad esta correcta, mediante la recuperación de la misma.

- SQL1.4: El aspecto a valorar será "¿Se mantiene un inventario actualizado de las versiones de SQL Server?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Prácticas recomendadas para revisar instancias" y podemos englobarla dentro de una acción de "Detección y enumeración de instancias, boletines y aplicación de revisiones". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Mantenga un inventario de todas las versiones, ediciones e idiomas de SQL Server de las que está a cargo; ii) Incluya las instancias de MSDE en el inventario; iii) Suscríbase a los boletines de seguridad de Microsoft; iv) Utilice SQL Scan y SQL Check (que puede obtener en el sitio Web de Microsoft) para buscar instancias de SQL Server en el dominio; v) Mantenga sistemas de prueba con la misma configuración que los sistemas de producción para poder probar en ellos las revisiones nuevas; vi) Pruebe las revisiones detenidamente antes de aplicarlas a los sistemas de producción; y vii) Considere la posibilidad de aplicar revisiones a sistemas de desarrollo sin realizar pruebas exhaustivas. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: No se mantiene un inventario actualizado de las versiones de SQL Server; y ii) Seguro: Se mantiene un inventario actualizado de las versiones de SQL Server. Este objetivo de control se valorara de forma "manual", y la prueba solicitada estará formada por los siguientes pasos: i) Solicitar un documento de control de versiones y en caso de existir verificar que es correcto; y ii) En caso de no existir el documento o no estar actualizado, se considerara que el objetivo de control no está cubierto.

- **Nivel Servidor:** Contiene los aspectos que afectan directamente a la configuración del servidor, sobre el que se encuentra implantado el SGBD. Estará formado por 3 aspectos valorables:
  - SQL2.1: El aspecto a valorar será "¿El servidor de BD tiene salida a Internet?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Configuración del entorno previo a la Instalación" y podemos englobarla dentro de una acción de "Servidores de Seguridad". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Instale un servidor de seguridad entre el servidor e Internet; ii) Bloquee siempre el puerto TCP 1433 y el puerto UDP 1434 en el servidor de seguridad perimetral. Si hay instancias con nombre que escuchan en otros puertos, bloquéelos también; y iii) En un entorno con varios niveles, utilice varios servidores de seguridad para crear subredes protegidas. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: El servidor de BD es accesible desde Internet; y ii) Seguro: El servidor de BD no es accesible desde Internet. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por los siguientes pasos: i) En caso de realizarla de forma manual se deberá abrir un navegador y verificar la salida a Internet poniendo una dirección web. En caso de realizarla de forma automática deberá lanzar una petición http contra una dirección web; y ii) Si existe conexión a Internet el sistema es Inseguro.
  - SQL2.2: El aspecto a valorar será "¿El servidor de BD es un controlador de dominios?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Configuración del entorno previo a la Instalación" y podemos englobarla dentro de una acción de "Aislamiento de servicios". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Aísle servicios para reducir el riesgo de que un servicio comprometido pueda utilizarse para comprometer otros servicios; ii) No instale nunca SQL Server en un controlador de dominio; iii) Ejecute servicios de SQL Server independientes con cuentas distintas de Windows; y iv) En un entorno con varios niveles, ejecute la lógica Web y la lógica de negocios en equipos independientes. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: El servidor de BD es un controlador de dominios; y ii) Seguro: El servidor de BD no es un controlador de dominios. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por los siguientes pasos: i) Obtendremos una lista de los usuarios del dominio: Net use > fichero.txt; y ii) Si detectamos peticiones de dominio de otros ordenadores los consideraremos inseguro.
  - SQL2.3: El aspecto a valorar será "¿El servidor de BD utiliza una partición NTFS?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Configuración del entorno previo a la Instalación" y podemos englobarla dentro de una acción de "Sistema de ficheros". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Utilice NTFS: Tanto los archivos de programa como las bases de datos deben residir en particiones NTFS y deben aplicarse las restricciones necesarias a nivel de sistema de archivos para evitar que, si por cualquier razón, alguien obtiene acceso al sistema, pueda cometer una catástrofe; ii) En la línea de comandos, escriba convert letra de la unidad: /FS:NTFS. Una unidad NTFS no se puede volver a convertir a FAT. Para obtener más información, consulte la documentación de Windows; y iii) Utilice RAID para archivos de datos esenciales. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: El servidor de BD no utiliza una partición NTFS; y ii) Seguro: El servidor de BD utiliza una partición NTFS. Este objetivo de control se valorara de forma "manual", y la prueba solicitada estará formada por los siguientes pasos: i) En el Explorador de Windows, seleccione la unidad y las pestaña de propiedades correspondientes. En la ficha General, se muestra el tipo de sistema de archivos; y ii) Si utilizar partición NTFS lo consideraremos seguro.

- **Nivel SGBD:** Contiene los aspectos que afectan directamente al Sistema de Gestión de Base de Datos. Estará formado por 26 aspectos valorables:
  - SQL3.1: El aspecto a valorar será "¿Existen archivos innecesarios creados durante la instalación?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Opciones de configuración tras las instalación" y podemos englobarla dentro de una acción de "Elimine o proteja archivos antiguos del programa de instalación". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Elimine o archive los siguientes archivos tras la instalación: sqlstp.log, sqlsp.log y setup.iss en la carpeta <unidadDelSistema>:\Archivos de programa\Microsoft SQL Server\MSSQL\Install en una instalación predeterminada y la carpeta <unidadDelSistema>:\Archivos de programa\Microsoft SQL Server\ MSSQL$<nombreDeInstancia>\Install en instancias con nombre; y ii) Si el sistema actual es una actualización de SQL Server 7.0, elimine los siguientes archivos: setup.iss en la carpeta %Windir% y sqlsp.log en la carpeta Temp de Windows. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Existen archivos innecesarios creados durante la instalación; y ii) Seguro: No existen archivos innecesarios creados durante la instalación. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por los siguientes pasos: i) Se mirara en el sistema de ficheros en las carpetas correspondientes si existen dichos archivos; y ii) Si existe algunos de dichos archivos el sistema se considerara Inseguro.
  - SQL3.2: El aspecto a valorar será "¿Están instalados las últimas actualizaciones y hotfixes, de SQL Server?", cuya responsabilidad recaerá sobre el

"Administrador del Sistema". El momento adecuado de valorar este aspecto es "Instalación" y podemos englobarla dentro de una acción de "Versión y Service Pack más recientes". La configuración correcta de este aspecto, requiere de cumplir el paso siguiente: i) Instale siempre los Service Pack y las revisiones de seguridad más recientes (Anexo II). Se han establecido tres valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: El servidor de BD tiene más de 5 actualizaciones no instaladas; ii) Inseguro: El servidor de BD tiene entre 1 y 5 actualizaciones no instaladas; y iii) Seguro: El servidor de BD tiene todas las actualizaciones instaladas. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por los siguientes pasos: i) La relación de actualizaciones aplicadas a SQL Server puede obtenerse ejecutando la orden *"xp_msver N'ProductVersion"*, y comparándola con las tablas del Anexo II; y ii) En caso de tener más de 5 parches sin instalar se considerará Muy Inseguro:. Entre 1 y 5 parches se considerará inseguro.

- SQL3.3: El aspecto a valorar será "¿Todas las instancias con nombres de SQL Server tienen puerto estáticos?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Opciones de configuración tras la instalación" y podemos englobarla dentro de una acción de "Escoja puertos estáticos para instancias con nombre". La configuración correcta de este aspecto, requiere de cumplir el paso siguiente: i) Asigne puertos estáticos a las instancias con nombre de SQL Server. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: No todas las instancias con nombres de SQL Server tienen puerto estáticos; y ii) Seguro: Todas las instancias con nombres de SQL Server tienen puerto estáticos. Este objetivo de control se valorara de forma "manual", y la prueba solicitada estará formada por los siguientes pasos: i) Ir a Herramientas de red del cliente => Alias y verificar que las instancias no tiene la opción de "puerto dinámico activado"; y ii) Si alguna instancia tiene puesto dinámicos se considerará Inseguro.
- SQL3.4: El aspecto a valorar será "¿La base de datos de ejemplo ha sido eliminada?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Opciones de configuración tras las instalación" y podemos englobarla dentro de una acción de "Elimine las bases de datos de ejemplo". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Elimine las bases de datos de ejemplo de los servidores de producción. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: La base de datos de ejemplo no ha sido eliminada; y ii) Seguro: La base de datos de ejemplo ha sido eliminada. Este objetivo de control se valorara de forma "manual o automático" utilizando el siguiente script *"select count(*) from sysdatabases where name='Northwind'"*, y la prueba solicitada estará formada por el siguiente paso: i) Verificar si existe la BD Nortwind.
- SQL3.5: El aspecto a valorar será "¿Se encuentran habilitadas las actualizaciones directas del catálogo?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Procedimientos administrativos periódicos recomendados" y podemos englobarla dentro de una acción de "Actualizaciones directas de catálogos". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) No permita las actualizaciones directas de catálogos. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: Se encuentran habilitadas las actualizaciones directas del catálogo; y ii) Seguro: No se encuentran habilitadas las actualizaciones directas del catálogo. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Propiedades del servidor => configuración del servidor => comportamiento del servidor. Y verificar si esta activada la opción de "Permitir que se modifiquen directamente los catálogos del sistema". La automatización podrá realizarse mediante la utilización del script *"select c.value from master.dbo.sysconfigures c, master..spt_values v, master.dbo.syscurconfigs r where v.type = 'C' and v.number = c.config and v.number >= 0 and v.number = r.config and (c.status & 2 = 0 or exists (select * from master.dbo.syscurconfigs where config = 518 and value = 1)) and name='allow updates' order by v.name"*.
- SQL3.6: El aspecto a valorar será "¿El nivel de auditoría establecido es "error" o "todo"?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Opciones de configuración tras la instalación" y podemos englobarla dentro de una acción de "Defina el nivel de auditoría de inicios de sesión y Control de acceso". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Establezca el nivel de auditoría de inicios de sesión en error o todo; y ii) Para habilitarlo, como administrador de SQL, ejecutar esto en el Query Analyzer: [xp_instance_regwrite N'HKEY_LOCAL_MACHINE',N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer',N'AuditLevel', REG_DWORD]. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: El nivel de auditoría establecido es distinto de "error" o "todo"; y ii) Seguro: El nivel de auditoría establecido es "error" o "todo". Este objetivo de control se valorara de forma "manual", y la prueba solicitada estará formada por el siguiente paso: i) Ir a propiedades del SGBD, pestaña de Seguridad y comprobar el Nivel de Auditoría activado.
- SQL3.7: El aspecto a valorar será "¿Las conexiones al SQL Server se realizan mediante la autenticación de Windows?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Instalación" y podemos englobarla dentro de una acción de "Modo de autenticación". La configuración correcta de este aspecto, requiere de cumplir el paso siguiente: i) Requiera la autenticación de Windows para las conexiones a SQL Server. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Menos del 30% de las conexiones al SGBD se realizan mediante la seguridad de Windows; y ii) Seguro: Las conexiones al SGBD se realizan mediante la seguridad de Windows. Se considerará seguro si entre un 0% y un 70% de los inicios de sesión totales se realizan mediante la seguridad de Windows. Este objetivo de control se valorara de forma "manual o automática", pudiendo automatizar mediante el script de la Tabla 4, y la prueba solicitada estará formada por el siguiente paso: i) Contamos cuantas cuentas dependen del S.O. y cuantas del SQL Server.

```
Select  cuentas_totales, cuentas_windows,
cuentas_sqlserver,
        100*convert(decimal(5,2),cuentas_windows) / convert(decimal(5,2),cuentas_totales)  as  porc_cuentas_windows,
        100*convert(decimal(5,2),cuentas_sqlserver)/ convert(decimal(5,2),cuentas_totales) as porc_cuentas_sqlserver
from ( select       count(*) as cuentas_totales,
                    sum(case isntname when 0 then 0 else 1 end) as cuentas_windows,
                    sum(case isntname when 0 then 1 else 0 end) as cuentas_sqlserver
        from syslogins) a
```

Tabla 4. Script para automatizar el control SQL3.7.

- SQL3.8: El aspecto a valorar será "¿El inicio de sesión "sa" tiene una contraseña segura?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Instalación y funcionamiento seguro" y

podemos englobarla dentro de una acción de "Contraseñas seguras y Proteja sa incluso en el modo de autenticación de Windows". La configuración correcta de este aspecto, requiere de cumplir el paso siguiente: i) Asigne siempre una contraseña segura a la cuenta de sa (administrador del sistema), incluso cuando se utilice la autenticación de Windows. Se han establecido tres valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: El inicio de sesión "sa" no tiene contraseña (NULL), o su contraseña es idéntica a su login; ii) Inseguro: El inicio de sesión "sa" tiene una contraseña poco segura, según los diccionarios utilizados; y iii) Seguro: El inicio de sesión "sa" tiene una contraseña segura. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada: Para verificar la seguridad de la contraseña se utilizarán diccionarios de fuerza bruta, que intentarán conectar mediante la generación de cadenas de odb: Generar cadenas de ODBC con login='sa' y password=''; ii) Generar cadenas de ODBC con login='sa' y password='sa; y iii) Generar cadenas de ODBC con login='sa' y password=[todas las palabras de los diccionarios]

- SQL3.9: El aspecto a valorar será "¿Existen contraseñas inseguras distintas del 'sa'?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Instalación y funcionamiento seguro" y podemos englobarla dentro de una acción de "Contraseñas seguras". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Utilice siempre contraseñas seguras para todas las cuentas de SQL Server; ii) Asigne una contraseña segura a la cuenta de 'sa', incluso en los servidores que están configurados para requerir la autenticación de Windows. Se han establecido tres valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: Existe algún inicio de sesión que no tiene contraseña (NULL), o su contraseña es idéntica a su login; ii) Inseguro: Existe algún inicio de sesión que tienen contraseñas poco seguras, según los diccionarios utilizados; iii) Seguro: Todos los inicios de sesión tienen contraseñas seguras. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por los siguientes pasos: i) Para verificar la seguridad de la contraseña se utilizarán diccionarios de fuerza bruta; ii) Mediante el siguiente script se puede verificar la existencia de cuentas sin contraseña *"Select name, Password from master.dbo.syslogins where password is null order by name"*; y iii) Para cada inicio de sesión diferente al 'sa': a) Generar cadenas de ODBC con login=[inicio_sesion] y password=''; b) Generar cadenas de ODBC con login=[inicio_sesion] y password=login; y c) Generar cadenas de ODBC con login=[inicio_sesion] y password=[todas las palabras de los diccionarios]
- SQL3.10: El aspecto a valorar será "¿Se realizan búsquedas periódicas de inicios de sesión con contraseñas no seguras?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Procedimientos administrativos periódicos recomendados" y podemos englobarla dentro de una acción de "Análisis de inicios de sesión". La configuración correcta de este aspecto, requiere de cumplir el paso siguiente: i) Realice búsquedas periódicas de cuentas con contraseñas NULL y quítelas o asígneles contraseñas seguras. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: No se realizan búsquedas periódicas de inicios de sesión con contraseñas no seguras. Existe alguna contraseña no segura, que no ha sido modificada desde hace más de 30 días; y ii) Seguro: Se realizan búsquedas periódicas de inicios de sesión con contraseñas no seguras. No existe ninguna contraseña no segura que no se hay modificado en los últimos 30 días. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Identificar contraseñas no seguras y ver desde cuando no se han modificado. Si

llevan más de 30 días sin modificarse, se considera que no hay revisión periódica. La automatización podrá realizarse mediante la utilización del script *"select name, datediff(dd,updatedate,getdate()) as dias_sin_modificar from syslogins order by accdate"*.

- SQL3.11: El aspecto a valorar será "¿Se eliminan los inicios de sesión que ya no se utilizan?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Procedimientos administrativos periódicos recomendados" y podemos englobarla dentro de una acción de "Análisis de inicios de sesión". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Elimine las cuentas que no se utilicen. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: No se eliminan los inicios de sesión que ya no se utilizan; y ii) Seguro: Se eliminan los inicios de sesión que ya no se utilizan. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el paso siguiente: i) Preguntar al administrador. La automatización podrá realizarse mediante la utilización del script *"select sid, name, datediff(dd,updatedate,getdate()) as dias_sin_modificar from syslogins order by accdate"*.
- SQL3.12: El aspecto a valorar será "¿Existen planes de seguridad y mantenimiento activados para las base de datos "master"?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Modelo y copias de seguridad". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Aprenda a trabajar con el modelo de seguridad de SQL Server; y ii) Realice copias de seguridad de todos los datos con regularidad y almacene las copias en una ubicación externa segura. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: No existen planes de seguridad y mantenimiento activados para las base de datos "master"; y ii) Seguro: Existen planes de seguridad y mantenimiento activados para las base de datos "master". Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) De forma automática se puede realizar atacando las tablas de la BD 'msdb'. Para realizarlo de forma manual ir a Administración, planes de mantenimiento de la BD y verificar si alguno de ellos incluye a la base de datos master. La automatización podrá realizarse mediante la utilización del script *"select count(*) from sysdbmaintplan_databases where database_name in ('All Databases','master')"*.
- SQL3.13: El aspecto a valorar será "¿Existen planes de seguridad y mantenimiento activados para las base de datos "msdb"?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Modelo y copias de seguridad". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Aprenda a trabajar con el modelo de seguridad de SQL Server; y ii) Realice copias de seguridad de todos los datos con regularidad y almacene las copias en una ubicación externa segura. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: No existen planes de seguridad y mantenimiento activados para las base de datos "msdb"; y ii) Seguro: Existen planes de seguridad y mantenimiento activados para las base de datos "msdb". Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el paso siguiente: i) De forma automática se puede realizar atacando las tablas de la BD 'msdb'. Para realizarlo de forma manual ir a Administración, planes de mantenimiento de la BD y verificar si alguno de ellos incluye a la base de datos msdb. La automatización podrá realizarse mediante

la utilización del script *"select count(*) from sysdbmaintplan_databases where database_name in ('All Databases','msdb')"*.

- SQL3.14: El aspecto a valorar será ¿Existen planes de seguridad y mantenimiento activados para las base de datos, diferentes de la "master" y "msdb"?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Modelo y copias de seguridad". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Aprenda a trabajar con el modelo de seguridad de SQL Server; y ii) Realice copias de seguridad de todos los datos con regularidad y almacene las copias en una ubicación externa segura. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Existe alguna Base de datos diferente de "master" y "msdb" que no tienen planes de seguridad y mantenimiento activados; y ii) Seguro: Existen planes de seguridad y mantenimiento activados para las base de datos. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) De forma automática se puede realizar atacando las tablas de la BD 'msdb'. Para realizarlo de forma manual ir a Administración, planes de mantenimiento de las BD. Mostraremos la lista de BD que no tienen planes de mantenimiento activados. La automatización podrá realizarse mediante la utilización del script *"select name from master.dbo.sysdatabases a where not exists (select database_name from msdb.dbo.sysdbmaintplan_databases b where a.name=b.database_name) and ('All Databases' not in (select database_name from msdb.dbo.sysdbmaintplan_databases))"*.
- SQL3.15: El aspecto a valorar será "¿Se analizan periódicamente los usuarios asociados a las funciones del servidor?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Procedimientos administrativos periódicos recomendados" y podemos englobarla dentro de una acción de "Enumere la pertenencia a funciones fijas". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Analice las funciones fijas de servidor y de base de datos de forma periódica para asegurarse de que sólo se permite la pertenencia a ellas a usuarios de confianza. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: Existen usuario/s con contraseña insegura asociados a funciones del servidor; y ii) Seguro: No se han encontrado usuario/s con contraseñas inseguras asociados a funciones del servidor. Este objetivo de control se valorara de forma "Manual o Automático", y la prueba solicitada estará formada por el siguiente paso: i) Identificar usuarios con contraseñas no seguras y ver a que funciones del servidor están asociados. Un usuario con contraseña inseguro nunca debería estar asociado a funciones del servidor. La automatización podrá realizarse mediante la utilización del script *"select sid, loginname, sysadmin+securityadmin+serveradmin+setupadmin+processadmin+diskadmin+dbcreator+bulkadmin from syslogins order by accdate"*.
- SQL3.16: El aspecto a valorar será "¿Cuantos usuarios son miembros de la función fija de servidor sysadmin?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Reducción de administradores". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Restrinja el número de miembros de la función fija de servidor sysadmin a unos pocos usuarios de confianza. Se han establecido tres valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: más de 50% de los usuarios son miembros de "sysadmin"; ii) Inseguro: 25% y el 50% de los usuarios son miembros de "sysadmin"; y iii) Seguro: 0% al 25% usuario son miembros de "sysadmin". Este objetivo de control se valorara de forma "Manual o Automático", pudiendo automatizarse mediante el script de la Tabla 5, y la prueba solicitada estará formada por el siguiente paso: i) Contar aquellos usuarios que tengan activados y reducirlo a un % del total.
- SQL3.17: El aspecto a valorar será "¿Existen restricciones de acceso para los procedimientos potencialmente peligrosos?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Procedimiento peligrosos". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Restringir el acceso a los procedimientos almacenados y procedimientos almacenados ampliados potencialmente peligrosos a únicamente los administradores de sistema (sysadmin). Se han establecido tres valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Al menos un procedimiento potencialmente peligroso puede ser ejecutado por miembros no pertenecientes a la función sysadmin; y ii) Seguro: Existen restricciones de acceso para los procedimientos potencialmente peligrosos. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Para cada uno de estos procedimientos mirar si tienen permisos alguien que no sea el administrador. La automatización podrá realizarse mediante la utilización del script *"select count(*) from sysusers a, sysprotects b, master.dbo.syslogins c where a.sid=c.sid and sysadmin=0 and a.uid=b.uid and id=object_id(N'[dbo].[xp_cmdshell]')"*.

```
select total_sid, sid_miembros_sysadmin, sid_nomiembros_sysadmin,
        100*convert(decimal(5,2),sid_miembros_sysadmin)/convert(decimal(5,2),total_sid) as porc_sid_miembros_sysadmin,
        100*convert(decimal(5,2),sid_nomiembros_sysadmin)/convert(decimal(5,2),total_sid) as porc_sid_nomiembros_sysadmin
 from ( select      count(*) total_sid,
                    sum(case sysadmin when 1 then 1 else 0 end) sid_miembros_sysadmin,
                    sum(case sysadmin when 1 then 0 else 1 end) sid_nomiembros_sysadmin
        from master.dbo.syslogins) a
```

Tabla 5. Script para automatizar el control SQL3.16.

- SQL3.18: El aspecto a valorar será "¿Esta deshabilitado el SQL Mail?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "SQL Mail". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Su utilización debe estar muy justificada y ser absolutamente imprescindible, ya que de estar activo estamos ofreciendo a un atacante potencial un nuevo mecanismo para la distribución de troyanos, virus o simplemente lanzar un ataque de denegación de servicio. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Esta habilitado el SQL Mail; ii) Seguro: No está habilitado el SQL Mail. Este objetivo de control se valorara de forma "Manual", y la prueba solicitada estará formada por los siguientes pasos: i) Ir a servicio de compatibilidad, SQL Mail, Propiedades y verificar si esta vinculado a algún servidor de correos.
- SQL3.19: El aspecto a valorar será "¿Se ha verificador la existencia de troyanos en master.sp_procoption?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "sp_procoption". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Comprobar que nadie haya dejado una puerta trasera. Son procedimientos que se arrancan automáticamente con el sistema. Se han establecido dos valores para realizar establecer el nivel de

cumplimiento del objetivo de control: i) Inseguro: Pueden existir troyanos; y ii) Seguro: No existen troyanos. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Solo debería existir el "Allow remote access". La automatización podrá realizarse mediante la utilización del script *"select count(*) from sysconfigures where status=0"*.

- SQL3.20: El aspecto a valorar será "¿Se ha verificador la existencia de troyanos en master.sp_password?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "sp_helpstartup". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Comprobar los scripts de las máquinas de producción con los scripts originales para determinar que no se ha realizado ningún cambio no autorizado. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: El código original del procedimiento es diferente al que existe en la actualidad; y ii) Seguro: Seguro: El código de sp_password no ha sufrido alteraciones. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) con el código del procedimiento sp_password adjunto (Anexo V).
- SQL3.21: El aspecto a valorar será "¿La gestión de permisos se hace a nivel de función o rol?", cuya responsabilidad recaerá sobre el "Administrador del Sistema y programador". El momento adecuado de valorar este aspecto es "Funcionamiento seguro y programación" y podemos englobarla dentro de una acción de "Funciones y grupos. Utilice funciones para simplificar la administración de permisos y la propiedad". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Agrupe los usuarios en funciones de SQL Server o en grupos de Windows para simplificar la administración de permisos; ii) Asigne permisos a funciones en lugar de asignarlos directamente a los usuarios; y iii) Puede hacer que los objetos pertenezcan a funciones, en lugar de pertenecer directamente a los usuarios, si desea evitar tener que modificar la aplicación cuando se quita el usuario propietario. Se han establecido tres valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: La gestión de los permisos se realiza a nivel de usuario. Existe menos de un 25% de los permisos de la BD que pertenecen a perfiles y no a usuarios; ii) Inseguro: La gestión de los permisos se realiza de forma mixta. Existe entre un 25%-75% de los permisos de la BD que pertenecen a perfiles y no a usuarios; y iii) Seguro: La gestión de los permisos se realiza a nivel de perfiles. Existe entre un 75%-100% de los permisos de la BD que pertenecen a perfiles y no a usuarios. Este objetivo de control se valorara de forma "Manual o Automático", pudiendo automatizarse utilizando el script de la Tabla 6, y la prueba solicitada estará formada por el siguiente paso: i) Verificar en la tabla syspermissions de cualquier BD, si los objetos a los que se han concedido permisos, son usuarios o roles.

```
Select total_permisos, total_permisos_roles, total_permisos_usuarios,
        100*convert(decimal(5,2),total_permisos_roles)/convert(decimal(5,2),total_permisos) as
porc_total_permisos_roles,
100*convert(decimal(5,2),total_permisos_usuarios)/convert(decimal(5,2),total_permisos) as
porc_total_permisos_usuarios
 from ( select      count(*) as total_permisos,
                    sum(case a.uid when a.gid then 1 else 0 end) as total_permisos_roles,
                    sum(case a.uid when a.gid then 0 else 1 end) as total_permisos_usuarios
        from sysusers a, syspermissions b
        where a.uid=b.grantee) a
```

Tabla 6. Script para automatizar el control SQL3.22.

- SQL3.22: El aspecto a valorar será "¿Tiene permisos la función de base de datos public?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Permisos". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) No otorgue nunca permisos a la función de base de datos **public**. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: La función public tiene permisos asignados; y ii) Seguro: La función public no tiene permisos asignados. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Verificar que la función de base de datos public no tiene permisos concedidos. La automatización podrá realizarse mediante la utilización del script *"select count(*) from sysusers a, syspermissions b where a.uid=b.grantee and a.name='public'"*.
- SQL3.23: El aspecto a valorar será "¿Existen servidores remotos para entornos con consultas distribuidas?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Consultas distribuidas". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Al instalar SQL Server en un entorno que admita las consultas distribuidas, utilice servidores vinculados en lugar de servidores remotos. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Existe algún servidor remoto para entornos con consultas distribuidas; y ii) Seguro: No existen servidores remotos para entornos con consultas distribuidas. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Mirar si existen servidores remotos en Seguridad => Servidores remotos. La automatización podrá realizarse mediante la utilización del script *"select count(*) from master.dbo.sysservers o where 1=1 and o.srvstatus & 32=0"*.
- SQL3.24: El aspecto a valorar será "¿Se gestionan los permisos a los servidores vinculados?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Consultas distribuidas". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Permita el acceso a los servidores vinculados sólo a los inicios de sesión que lo necesitan. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Existe algún servidor vinculado sin el control adecuado de seguridad; y ii) Seguro: Se gestionan los permisos de los servidores vinculados. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Mirar si existen servidores remotos en Seguridad => Servidores vinculados => Propiedades => Seguridad. La automatización podrá realizarse mediante la utilización del script *"select count(*) from master.dbo.sysservers where srvstatus & 32 <> 0 and providerstring is null"*.
- SQL3.25: El aspecto a valorar será "¿Se controlan los accesos fallidos a la aplicación?", cuya responsabilidad recaerá sobre el "Administrador del Sistema". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Control de acceso". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Programar una tarea que los controle: findstr /C:"Login Failed" \[vía acceso SQL]\log*.*; y ii) Redireccionar la salida a un archivo y enviarlo por correo para poder monitorizar los intentos no satisfactorios de conexión. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: No se controlan los accesos fallidos al SGBD; y ii) Seguro: Se con-

trolan los accesos fallidos al SGBD. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Realizar un acceso fallido a la aplicación y verificar si en la ruta indicada a quedado algún registro. La automatización podrá realizarse mediante la utilización del script *"findstr /C:"Login Failed" \[vía acceso SQL]\log*.*"*.

- SQL3.26: El aspecto a valorar será "¿Se utiliza la cuenta de "sa" para enviar datos al SGBD?", cuya responsabilidad recaerá sobre el "Programador". El momento adecuado de valorar este aspecto es "General" y podemos englobarla dentro de una acción de "Evite el acceso a SQL". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) Protéjase contra el acceso a SQL mediante la validación de todos los datos introducidos por el usuario antes de transmitirlos al servidor; ii) Para limitar el alcance de los posibles daños, permita enviar datos introducidos por el usuario al servidor sólo a las cuentas con los menores privilegios; y iii) Ejecute SQL Server con el menor número posible de privilegios. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Utiliza la cuenta "sa" para enviar datos al servidor; y ii) Seguro: No utiliza la cuenta "sa" para enviar datos al servidor. Este objetivo de control se valorara de forma "manual", y la prueba solicitada estará formada por el siguiente paso: i) Activar una auditoría de transacciones con el SQL Profiler y verificar si la cuenta utilizada para transacciones externas es 'sa'.

- **Nivel BD:** Contiene los aspectos que afectan directamente a las Bases de Datos. Estará formado por 4 aspectos valorables:
  - SQL4.1: El aspecto a valorar será "¿Se utiliza código embebido en las objetos de la BD?", cuya responsabilidad recaerá sobre el "Programador". El momento adecuado de valorar este aspecto es "General" y podemos englobarla dentro de una acción de "Control del código". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Protéjase contra el acceso a SQL mediante el desarrollo de una programación estructurada. Se han establecido tres valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Muy Inseguro: No se utiliza nunca código embebido en las objetos de la BD; ii) Inseguro: Se utiliza un modo mixto, parte del código esta embebido y parte es externo; y iii) Seguro: Se utiliza código embebido en las objetos de la BD. Este objetivo de control se valorara de forma "Manual", y la prueba solicitada estará formada por el siguiente paso: i) Activar una auditoría de transacciones con el SQL Profiler y verificar si las transacciones externas se realizan directamente sobre los objetos bases (tablas) o utilizan objetos intermedios.
  - SQL4.2: El aspecto a valorar será "¿Se utiliza vistas para minimizar las dependencias entre BD?", cuya responsabilidad recaerá sobre el "Programador". El momento adecuado de valorar este aspecto es "General" y podemos englobarla dentro de una acción de "Control del código". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Protéjase contra el acceso a SQL mediante el desarrollo de una programación estructurada. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Existen dependencias entre BD que no están contenidas en vistas; y ii) Seguro: Se utilizan vistas para minimizar las dependencias entre BD. Este objetivo de control se valorara de forma "manual o automática", pudiendo automatizarse mediante el script de la Tabla 7, y la prueba solicitada estará formada por el siguiente paso: i) Analizar las dependencias con servidores vinculados y verificar el tipo de objetos que las contienen. Usar para ellos las tablas sysservers, sysobjects, syscomments.


```
select srvname collate SQL_Latin1_General_CP1_CI_AS from
master.dbo.sysservers
declare @servidor varchar(128)
select @servidor = ''
select   total, servidor_novista, servidor_vista,
        case when total=0 then 0 else 100*convert(deci-
mal(9,2),servidor_novista)/convert(decimal(9,2),total) end as
porc_servidor_novista,
        case when total=0 then 0 else 100*convert(deci-
mal(9,2),servidor_vista)/convert(decimal(9,2),total) end as
porc_servidor_vista
from (  select      count(*) as total,
                    isnull(sum(case when xtype='V' then 1 else
0 end),0) servidor_vista,
                    isnull(sum(case when xtype='V' then 0 else
1 end),0) servidor_novista
        from sysobjects a, syscomments b
        where text like '%'+@servidor+'%') a
```

Tabla 7. Script para automatizar el control SQL4.2.

o SQL4.3: El aspecto a valorar será "¿Se utiliza la encriptación de los procedimientos?", cuya responsabilidad recaerá sobre el "Programador". El momento adecuado de valorar este aspecto es "General" y podemos englobarla dentro de una acción de "Control del código". La configuración correcta de este aspecto, requiere de cumplir el siguiente paso: i) Protéjase contra el acceso no autorizado al código SQL embebido. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: Menos del 75% de los objetos embebidos se encuentran encriptados; ii) Seguro: La mayor parte del código embebido esta encriptado. Más del 75% del código. Este objetivo de control se valorara de forma "Manual", aunque podrá automatizarse utilizando el script de la Tabla 8, y la prueba solicitada estará formada por el siguiente paso: i) Ver qué porcentaje de los objetos de la base de datos se encuentran encriptados. Se aconseja que durante la fase de desarrollo se creen los objetos con la línea "/* with Encryption */" y al pasarla a producción se reemplace por la línea " with Encryption ", con lo que los códigos de la aplicación quedarán protegidos

```
select   total, objetos_noencriptados, objetos_encriptados,

100*convert(decimal(9,2),objetos_noencriptados)/convert(d
ecimal(9,2),total) as porc_objetos_noencriptados,
        100*convert(decimal(9,2),objetos_encriptados)/con-
vert(decimal(9,2),total) as porc_objetos_encriptados
from (select        count(*) as total,
                    sum(case when encrypted=0 then 1 else 0
end) objetos_noencriptados,
                    sum(case when encrypted=0 then 0 else 1
end) objetos_encriptados
        from sysobjects a, syscomments b
        where a.id=b.id and xtype in ('FN','IF','P','TR','V')) a
```

Tabla 8. Script para automatizar el control SQL4.3.

o SQL4.4: El aspecto a valorar será "¿La cuenta de invitado (guest) esta deshabilitada?", cuya responsabilidad recaerá sobre el "Administrador de Sistemas". El momento adecuado de valorar este aspecto es "Funcionamiento seguro" y podemos englobarla dentro de una acción de "Cuentas de guest". La configuración correcta de este aspecto, requiere de cumplir los siguientes pasos: i) No habilite la cuenta de guest; ii) Con el objetivo de prevenir el acceso no autorizado a los datos, el acceso deberá realizarse siempre mediante usuarios autenticados. Como excepción a esta regla debe indicarse que las bases de datos master y tempdb requieren la cuenta de usuario invitado. Se han establecido dos valores para realizar establecer el nivel de cumplimiento del objetivo de control: i) Inseguro: La cuenta de invitado está habilitada; ii) Seguro: La cuenta de invitado esta deshabilitada. Este objetivo de control se valorara de forma "manual o automática", y la prueba solicitada estará formada por el siguiente paso: i) Verificamos que la cuenta Guest no está creada. La automatización podrá realizarse mediante la utilización del script *"select count(*) from sysusers where name='guest'"*.