ÍNDICE

ALCANCE

El Diccionario de Datos o Repositorio de una aplicación, proyecto, etc. Consiste en una Base de Datos o Catálogo de los propios datos de la aplicación a la que pertenece. Por tanto guarda información imprescindible para el funcionamiento de dicha aplicación y para su uso, o en el caso de un proyecto para el desarrollo del mismo, de ésta forma damos la importancia que se merece al Repositorio y así en los objetivos destacaremos los aspectos fundamentales de la seguridad.

OBJETIVO

Dada la importancia de los datos incluidos en un Repositorio, se han de establecer unas normas y conductas de utilización y mantenimiento del Repositorio para evitar posibles fallos en su funcionamiento. Los aspectos más destacados los resumiríamos en estos puntos:

- **Fallo en la máquina o servidor que sostiene el Repositorio.**
- **Fallo en las comunicaciones con la Base de Datos.**
- **Inconsistencias en los datos.**
- **Pérdida de datos.**
- **Accesos no autorizados.**
- **Todo tipo de modificaciones no autorizadas.**
- **Copias diarias de seguridad.**
- **Bloqueos para modificaciones.**
- **Documentación y Ficheros Log de todos los cambios realizados.**
- **Seguimiento de una política de actualización.**
- **...**

METODOLOGÍA CHECKLIST

Metodología basada en Riesgo vs. Control vs. Coste. El auditor revisa o audita los controles con la ayuda de una lista de control (checklist) que consta de una serie de preguntas o cuestiones a verificar. La evaluación consiste en identificar la existencia de unos controles establecidos.

Las listas de control suelen utilizarse por los auditores, generalmente por auditores con poca experiencia, como una guía de referencia, para asegurar que se han revisado todos los controles.

En nuestro caso particular se ha dividido la lista de control en los siguientes apartados:

- **Conocimiento del sistema:**

- **Inventario**
- **Software**
- **Pruebas**
- **Planes de contingencia**

- **Repositorio**

- **Seguridad**
- **Proceso de cambio**

CHECKLIST DEL DICCIONARIO DE DATOS	*SÍ*	*NO*	*N/A*
CONOCIMIENTO DEL SISTEMA: INVENTARIO			
¿Hay un inventario en la compañía de Sistemas, Hardware y Datos?			
¿Ha hecho revisar el inventario por un especialista (auditor, consultor, experto en informática...) *externo a la empresa*?			
¿Se sabe quiénes son los propietarios de los elementos del inventario?			
¿Se sabe quiénes son los usuarios de los elementos del inventario?			
¿Existe un criterio para valorar cuáles son los elementos críticos del inventario?			
¿Se distingue en ese criterio entre: Riesgos para el negocio, riesgos para el servicio prestado a los clientes y riesgo de parálisis de la gestión de la Compañía?			
¿Han validado ese criterio los jefes de Gestión de la Empresa y los jefes de Informática?			
¿Se ha realizado, por lo tanto, un ranking de los elementos más críticos?			
¿Se van a comenzar las pruebas y actualizaciones, por lo tanto, siguiendo el orden del ranking?			
	SÍ	*NO*	*N/A*
CONOCIMIENTO DEL SISTEMA: SOFTWARE			
¿Ha tenido en cuenta las distintas versiones de los elementos Software?			
¿Es posible modificar y mejorar el código fuente de sus programas a medida?			
¿Está disponible el código fuente?			
¿Se han hecho estudios coste/beneficio sobre si cambiar los sistemas del departamento o mejorarlos?			
¿ Se han hecho estudios que revelan cuál es la manera más sencilla y menos costosa de cambiar y mejorar el sistema?			
¿Ha identificado qué códigos fuente son propiedad de otras entidades?			
¿Existe un contrato de utilización con los propietarios?			
¿Va a exigirles a los propietarios de dichos códigos un informe de progresos?			
¿Tiene asesoramiento legal para asegurarse de que dichos contratos			

son correctos y puede exigir compensaciones económicas en caso de incumplimiento?			
	SÍ	***NO***	***N/A***
¿Ha verificado en general los productos adquiridos recientemente?(contratos de utilización, códigos fuente,...)			
¿Su suministrador de software sigue el negocio?			
CONOCIMIENTO DEL SISTEMA: PRUEBAS			
¿Se van a someter los elementos más críticos a unas pruebas especiales?			
¿Va a usar un Software especial para ello?			
¿Va a contratar los servicios de un especialista (auditor, consultor, experto en informática...) externo a la empresa para ello?			
A la hora de verificar los elementos más críticos, ¿Se asegura que no dependen de otros situados en un estrato menor del ranking?			
¿Han verificado, en ese caso, ambos elementos a la vez?			
¿Ha decidido, en función del ranking, qué datos probar y en qué orden?			
	SÍ	***NO***	***N/A***
¿Va a utilizar un software especial para ello?			
¿Ha sido validado dicho software por auditores?			
¿Tiene el equipo del proyecto un plan de prueba que incluya, al menos, una especificación del tipo de pruebas, la fecha de comienzo de las pruebas, los recursos (de hardware, humanos y tiempo) para realizar las pruebas y la especificación de los casos de pruebas satisfactorias?			
¿Los responsables de realizar las pruebas tienen la formación adecuada?			
Si es necesario probar datos confidenciales, ¿se asegura que sean ficticios o no relevantes, y si deben ser reales, se asegura que sean eliminados después de la prueba?			
Si no es posible eliminar datos confidenciales usados en las pruebas, ¿se asegura que sólo algunos empleados tienen autoridad y acceso para hacer las pruebas y que están debidamente registrados todos los accesos que realizan?			
CONOCIMIENTO DEL SISTEMA: PLANES DE CONTINGENCIA			
¿El personal de la organización sabe que tiene soporte si ocurren problemas?			
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento del Repositorio o Diccionario de Datos?			
	SÍ	***NO***	***N/A***
¿En el plan se identifican todos los riesgos y sus posibles alternativas?			
REPOSITORIO: SEGURIDAD			
¿Existe un administrador de sistemas que controle a los usuarios?			
¿Gestiona los perfiles de los usuarios dicho administrador?			
¿Existe un administrador de bases de datos que gestione las instancias de las bases de datos?			

¿Gestiona el administrador de bases de datos los accesos a las distintas instancias de las bases de datos?			
¿Existe un acceso restringido a las instancias que contienen el Repositorio?			
¿Es autocambiable la clave de acceso al Repositorio?			
¿Pueden los administradores del Repositorio cambiar la contraseña?			
¿Se obliga, cada cierto tiempo, a cambiar la contraseña automáticamente?			
¿Se renueva periódicamente la contraseña?			
	SÍ	***NO***	***N/A***
¿Existen listados de intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?			
¿Existe un diseño físico y lógico de las bases de datos?			
¿Dispone también el Diccionario de datos de un diseño físico y lógico?			
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?			
¿Está restringido el acceso al entorno de desarrollo?			
¿Se utilizan datos reales en el entorno de desarrollo?			
¿Existen copias de seguridad del Repositorio?			
¿Se hacen copias de seguridad diariamente?			
¿Se almacenan las copias de seguridad en dispositivos externos?			
¿Se ubican los dispositivos externos en locales diferentes al edificio en el que se encuentran las redes y los servidores?			
	SÍ	***NO***	***N/A***
¿Existe un acceso restringido a la sala de servidores?			
¿Existen mecanismos de seguridad física en las salas de servidores?			
¿Se dispone de equipos auxiliares en caso de caída o avería del equipo principal?			
¿Se dispone de generador de energía auxiliar para asegurar la corriente a los servidores?			
REPOSITORIO: PROCESO DE CAMBIO			
¿Existe un formulario de petición de cambio o modificación en el Repositorio?			
¿Es necesaria la autorización del Manager del Repositorio para realizar el cambio?			
¿Se realiza la modificación sobre una copia del Repositorio?			
¿Se establece un bloqueo sobre la parte del Repositorio a modificar?			
¿Se comunica a los distintos usuarios/desarrolladores el bloqueo de parte del Repositorio y por tanto los fallos del funcionamiento que se pueden ocasionar?			
¿Se establecen prioridades en los trabajos y modificaciones del repositorio para los bloqueos?			
	SÍ	***NO***	***N/A***
¿Existe algún fichero log que almacene todos los cambios realizados en el Repositorio?			

¿Se comunica al solicitante del cambio que se ha llevado a cabo la modificación?
¿Se realizan pruebas sobre el cambio para comprobar que la aplicación funciona correctamente?
¿Se comprueba que el cambio solicitado se corresponde con lo realizado?
¿Se realizan dichas comprobaciones en la copia de la instancia?
¿Existe una notificación por escrito del solicitante certificando que el cambio se realizó satisfactoriamente?
¿ Existe documentación escrita sobre el cambio (formulario de petición, script del cambio realizado, aprobación del solicitante)?
¿Se realiza un volcado de la copia del Repositorio el original al final del dia?
¿Se realizan actualizaciones periódicamente del resto de las instancias para que tengan el Diccionario de Datos actualizado?

CONCLUSIÓN

A la vista de los resultados obtenidos al realizar el Checklist, podremos comprobar la existencia de los procedimientos, normas y conductas de seguridad necesarias para un buen mantenimiento del Repositorio para evitar posibles fallos en el funcionamiento de las aplicaciones e inclusive fallos catastróficos para el negocio, para la empresa y sus clientes.

BIBLIOGRAFÍA

Análisis y diseño detallado de Aplicaciones Informáticas de Gestión

Mario Piattini, J. Antonio Calvo−Manzano, Joaquín Cervera, Luis Fernández.

Coeditorial: Alfaomega−Rama. Ed 1999

Apuntes de Auditoría Informática de la Universidad Pontificia de Salamanca en Madrid Curso 1999−2000

Carlos M. Fernández Sanchez.

IV Jornadas de Ingeniería del Software y Bases de Datos

24−26 Noviembre 1999. Cáceres. (consultado vía Internet)

EDR DE UN PC

RIESGO	OBJETIVO DE CONTROL	CONTROLES	PRUEBA DE CUMPLIMIENTO	PRUEBA SUSTANTIVA
Quedarse falto de memoria en poco tiempo	El equipo no se quede anticuado y se pueda ampliar	Ordenador tenga más ranuras de expansión	Abrir el ordenador y comprobrarlo visualmente	Comprobación física. Poner Memoria adicional, Colocar otro disco duro y comprobar su funcionamiento

Quedarse falto de espacio en disco duro en poco tiempo		Tenga espacio y cableado para los discos duros		
Quedarse con un procesador anticuado		Tener una placa base ampliable		
Deterioro del PC: humedad, polvo, interferencias con otros aparatos electricos	Proteger el PC contra causas externas	Ubicación adecuada del PC, Fundas para monitor y teclado, Enchufes específicos para el PC	Comprobar y revisar que las fundas están bien puestas y que los enchufes sean únicos para el PC	
Utilización del PC por personas no autorizadas	Proteccion de la información del ordenador	Llave de bloqueo del teclado	Comprobar que sin la llave no se puede usar el teclado	Tener la llave a buen recaudo
		Password al inicio de sesión	Verificar que la contraseña es válida	Tener la contraseña a buen recaudo
Pérdida o modificación de información debido a personas no autorizadas		Establecer password y atributos de solo lectura en los archivos que lo requieran	Verificar los atributos y las contraseñas	
Pérdida de la configuración actual del PC	Proteccion dela configuración del PC	Establecer una password a la BIOS	Verificar y tener apuntado la contraseña	
Pérdiad de información debido a los virus	Asegurar la integridad de los datos	Poseer un antivirus y renovarlo asiduamente	Comprobar que se ejecuta el antivirus cada vez que se arranca el PC y cuando se inserta un disquete	Funcionamiento del antivirus en caso real
		Realizar backup's cada cierto tiempo : streamer, Cd−Rom, ...	Verificar que los datos almacenados en soporte externo pueden utilizarse	
Deterioro del Disco Duro (Clusters erroneos, ocupación del disco sin seguir un orden, ...)	Pérdida de información	Escanear el PC cada cierto tiempo	Comprobar que el planificador de tareas realiza la verificación del disco duro	

Bajo rendimiento del PC	Optimización de los recursos	Utilizar un Programa que realice la optimización	Comprobar que los recursos están optimizados al máximo	

5

1

5

5