SERIE OCDE SUR LES PRINCIPES DE BONNES PRATIQUES DE LABORATOIRE ET LA VERIFICATION DU RESPECT DE CES PRINCIPES
NUMERO 10
OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING
NUMBER 10

Ceci est la traduction en espagnol du même document déjà diffusé en anglais et en français.

This is the Spanish translation of this document which has already been distributed in English and in French.

ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Paris

71988

SERIE DE LA OCDE ACERCA DE LOS PRINCIPIOS DE BUENAS PRÁCTICAS DE LABORATORIO Y VERIFICACIÓN DE SU CONFORMIDAD

Número 10

Documento de Consenso sobre BPL

APLICACIÓN DE LOS PRINCIPIOS DE BPL A LOS SISTEMAS INFORMÁTICOS

MONOGRAFÍA MEDIOAMBIENTAL Nº 116

Dirección de Medio Ambiente

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO

París 1995

PREFACIO

Con motivo del tercer Taller de Consenso de la OCDE relativo a las buenas prácticas de laboratorio, que tuvo lugar los días 5 al 8 de octubre de 1992 en Interlaken (Suiza) un grupo de expertos procedió al examen de la interpretación de los Principios de BPL aplicados a los sistemas informáticos. El Grupo de expertos estuvo presidido por el Señor Theo Helder, representante de la Autoridad holandesa de verificación de BPL. El ponente, fue el Señor Brian Doherty (Presidente de la Comisión Informática de la Asociación británica relativa al aseguramiento de la calidad en el sector de la investigación (BARQA). Los participantes en el Grupo de trabajo estaban representados por algunas autoridades nacionales de verificación en el aspecto de BPL y en otros casos, de los laboratorios de pruebas de los países siguientes: Alemania, Austria, Bélgica, Dinamarca, Estados Unidos de América, Finlandia, Francia, Holanda, Japón, Reino Unido y Suiza. El Grupo de expertos no pudo, por falta de tiempo, llegar a un consenso relativo a un documento de orientación detallado, pero no obstante, elaboró un documento que lleva por título "Aplicación de los principios de BPL a los sistemas informáticos", en el cual se recogen los Principios generales y se describen los puntos derivados de cada uno. Este documento se ha distribuido a los países Miembros para que formulen sus comentarios correspondientes.

Tomando como punto de partida las observaciones formuladas, la Comisión sobre Buenas Prácticas de Laboratorio, llegó a la conclusión, durante su quinta reunión de marzo de 1993 por la cual otros trabajos serían necesarios y que el Grupo de trabajo debería reunirse una segunda vez. El Grupo se reunió en París los días 14 al 16 de diciembre de 1994, bajo la presidencia del Señor Doherty con la participación del Señor Doherty a título de ponente. Estuvieron presentes en esta reunión los representantes de los gobiernos y de la industria de Alemania, Canadá, Dinamarca, Estados Unidos de América, Francia, Holanda, Japón, Reino Unido y Suecia.

El proyecto de documento de Consenso elaborado por el Grupo de expertos tiene como fundamento el documento procedente de la reunión de Interlaken, los comentarios formulados por los países Miembros con este motivo y un documento elaborado por un Grupo de trabajo conjunto Gobierno/industria del Reino Unido. Este documento fue sometido seguidamente a examen y modificado y aprobado por la Comisión sobre las BPL y la Reunión conjunta del Grupo de productos químicos y del Comité de gestión del Programa especial relativo al control de los productos químicos. El Comité de políticas medioambientales recomendó, acto seguido, que el presente documento fuese publicado bajo la autoridad del Secretario General.

DOCUMENTO DE CONSENSO SOBRE BPL: APLICACIÓN DE LOS PRINCIPIOS DE BPL A LOS SISTEMAS INFORMÁTICOS

Se ha observado recientemente que la utilización de los sistemas informáticos se ha desarrollado en las instalaciones de pruebas que llevan a cabo ensayos de inocuidad para la salud y el medio ambiente. Estos sistemas informáticos pueden permitir, directa o indirectamente, la integración, el procesamiento, la presentación y almacenamiento de datos y se encuentran, cada vez más, integrados frecuentemente en los equipos automatizados. Cuando estos sistemas informáticos se encuentran combinados con la ejecución de estudios llevados a cabo con fines normativos, su concepto, su validación, su operación y su mantenimiento deberán guardar conformidad con los Principios de Buenas Prácticas de Laboratorio de la OCDE.

Sector de aplicación

Todos los sistemas informáticos que se utilizan para producir, medir o evaluar los datos con fines normativos deberán estar proyectados, validados, operados y administrados con el debido respeto de los Principios de BPL.

Para la planificación, la ejecución y la presentación de los resultados de los estudios se pueden utilizar diversos sistemas informáticos. Estos sistemas se pueden aplicar para adquirir, directa o indirectamente, los datos registrados por medio de los equipos automatizados, operar/controlar los equipos automatizados y finalmente, procesar, presentar y almacenar los datos. Los sistemas informáticos utilizados para tales actividades pueden ser de diversa índole y pueden incluir desde los instrumentos de análisis programables o un ordenador personal, hasta un sistema de gestión de las informaciones del laboratorio (LIMS) de funciones múltiples. Los Principios de BPL deberán ser aplicados sea cual fuere el grado de intervención del ordenador.

Método

Los sistemas informáticos, asociados a la ejecución de los estudios llevados a cabo con fines normativos, deberán corresponder a un concepto adecuado, disponer de una capacidad suficiente y ser convenientes para las tareas a las cuales están destinados. Los procedimientos adecuados se deberán proyectar para controlar y administrar estos sistemas, que deberán también estar proyectados, validados y operados de conformidad con los Principios de BPL.

También desempeña un papel determinante la operación denominada "de validación", que permite demostrar que un sistema informático está adaptado a las tareas para las cuales se destina.

El procedimiento de validación presenta las suficientes garantías para poder permitir que un sistema informático responda al pliego de condiciones establecidas. La validación debe corresponder al marco de un programa oficial de validación y se deberá ejecutar antes de la puesta en servicio del sistema.

APLICACIÓN DE LOS PRINCIPIOS DE BPL A LOS SISTEMAS INFORMÁTICOS

Las consideraciones que figuran a continuación habrán de facilitar la aplicación de los Principios de BPL a los sistemas informáticos que se describen a continuación.

1. Responsabilidades

a) La *dirección* de la instalación de pruebas asume la responsabilidad general de la aplicación de los Principios de BPL. Fundamentalmente, corresponde a esta Dirección seleccionar un número adecuado de personas suficientemente cualificadas y experimentadas y, asimismo, organizar eficazmente su trabajo, así como velar para que las instalaciones, los equipos y los procedimientos de gestión de datos correspondan a las normas requeridas.

La Dirección tiene a su cargo supervisar que los sistemas informáticos convengan a las tareas para las cuales están destinados. Así, deberá definir las instrucciones y procedimientos informáticos para garantizar que los sistemas están proyectados, validados, operados y mantenidos de conformidad con los Principios de BPL. La Dirección tendrá también a su cargo velar que estas instrucciones y procedimientos se han comprendido y observado y, asumirá el control efectivo de la aplicación de estas disposiciones.

La Dirección debe también contratar personal encargado específicamente del desarrollo, de la validación, de la operación y del mantenimiento de los sistemas informáticos. Este personal deberá tener la calificación suficiente y poseer una correcta experiencia, y asimismo, haber recibido una capacitación adecuada para asumir las tareas que le son encargadas con el debido respeto de los Principios de BPL.

b) Los *directores de estudio* tienen a su cargo la responsabilidad, siempre en aplicación de los Principios de BPL, de la dirección general de sus estudios. Habida cuenta que estos estudios habrán de recurrir frecuentemente a los sistemas informáticos, resulta indispensable que los Directores de los estudios estén perfectamente al tanto de la utilización de cualquier sistema informático que intervenga en los estudios que se llevan a cabo bajo su dirección.

Al tratarse de los datos registrados por medios electrónicos, la responsabilidad del director de estudio es la misma que cuando se trata de los datos registrados en papel y, por consiguiente, únicamente los sistemas validados se podrán utilizar en los estudios relativos a las BPL.

c) *Personal*. La totalidad del personal que utiliza sistemas informáticos deberá operar estos sistemas con el debido respeto de los Principios de BPL. Así, corresponderá al personal encargado de desarrollar, validar, operar los sistemas informáticos y asumir su mantenimiento, llevar a cabo estas actividades de conformidad con los Principios de BPL y de las normas técnicas reconocidas.

d) Las responsabilidades en el aspecto del *aseguramiento de la calidad* (AC) de los sistemas informáticos habrán de ser definidas por la Dirección y descritas en instrucciones y procedimientos impartidos por escrito. El programa de aseguramiento de la calidad deberá comprender los procedimientos y las prácticas que permitan garantizar el debido respeto de las normas establecidas en todas las etapas de la validación, de la operación y del mantenimiento de los sistemas informáticos. Además, incluirá los procedimientos y prácticas para la introducción de los sistemas adquiridos y para la adaptación de sistemas informáticos a las necesidades internas.

El personal encargado del aseguramiento de la calidad habrá de verificar si los sistemas informáticos guardan conformidad con las BPL y deberá recibir la capacitación técnica especializada que la situación así lo exige. Deberá conocer suficientemente estos sistemas para poder formular comentarios

objetivos ; en ciertos casos, será conveniente recurrir a auditores especializados en sistemas de aseguramiento de la calidad.

El personal encargado del aseguramiento de la calidad deberá tener acceso, únicamente en lectura a los datos almacenados en los sistemas informáticos para su control.

2. Capacitación

Para responder a los Principios de BPL, las instalaciones de pruebas deberán emplear personal cualificado y experimentado y aplicar programas de capacitación detallados, que incluyan las capacitaciones para el puesto de trabajo y, llegado el caso, cursos impartidos por parte de organismos externos. Se deberán conservar las documentaciones relativas a estas capacitaciones.

Las disposiciones anteriores se habrán de aplicar a la totalidad del personal que participa en la utilización de los sistemas informáticos.

3. Instalaciones y equipos

Se deberá disponer de instalaciones y equipos adecuados para garantizar la correcta ejecución de los estudios, siempre de conformidad con los principios de BPL. Al tratarse de los sistemas informáticos, se deberán tener en cuenta cierto número de aspectos específicos:

a) Instalaciones

Se deberá proceder a un estudio detallado del emplazamiento de los equipos, de los elementos periféricos, de los equipos de comunicación y de los sistemas electrónicos de almacenamiento. Se deberán evitar las fuertes variaciones de temperatura y de humedad, el polvo, las interferencias electromagnéticas y la proximidad de cables de alta tensión, salvo si el equipo está especialmente proyectado para funcionar en semejantes condiciones.

También se deberá estudiar la alimentación eléctrica de los equipos informáticos, sin perder de vista llegado el caso, una alimentación de emergencia y sin interrupciones para los sistemas informáticos cuya interrupción repentina podría alterar los resultados de un estudio.

También se tendrán en cuenta los equipos adecuados para garantizar la seguridad del soporte electrónico de informaciones.

b) Equipo

i. Hardware y software

Un sistema informático constituye un grupo de elementos materiales y softwares, proyectado y ensamblado para llevar a cabo una función o un grupo de funciones determinadas.

El hardware constituye la parte física del sistema informático y está formado por la unidad central del ordenador y sus periféricos.

El software corresponde a el, o los programa(s) necesario(s) para la operación del sistema informático.

Todos los Principios de BPL aplicables a los equipos tienen también, por consiguiente, aplicación al hardware y al software.

ii. Comunicaciones

Las comunicaciones asociadas a los sistemas informáticos corresponden, en su sentido más amplio, a dos categorías: efectivamente, pueden poner en comunicación entre sí a varios ordenadores, o bien a los ordenadores y sus sistemas periféricos.

Todos los sistemas de intercomunicación pueden constituir fuentes potenciales de errores y pueden acarrear la pérdida o la alteración de los datos. Se deberán tener en cuenta las medidas de control adecuadas para garantizar la seguridad y la integridad de los sistemas en el momento del diseño, de la validación, de la operación y del mantenimiento de cualquier sistema informático.

4. Mantenimiento y Recuperación tras un fallo o incidente

Todos los sistemas informáticos se deberán instalar y mantener con objeto de garantizar un correcto funcionamiento de forma permanente.

a) Mantenimiento

Se deberá disponer de procedimientos establecidos por escrito que describan el mantenimiento preventivo corriente y la reparación de los fallos. Estos procedimientos deberán definir claramente los cometidos y las responsabilidades del personal correspondiente. Cuando estas actividades de mantenimiento han dado lugar a una modificación del hardware y/o del software, podrá ser necesario validar de nuevo el sistema. Todos los problemas y anomalías detectados durante la operación del sistema, así como las medidas correctivas aplicadas, se deberán consignar por escrito diariamente.

b) Recuperación tras un fallo o incidente

Será preciso disponer de procedimientos que describen las medidas que cabe tomar en caso de fallo parcial o completo de un sistema informático. Estas medidas pueden dar comienzo por la redundancia planificada de ciertos equipos y, finalizar por un retorno al sistema sobre soporte papel. Todos los planes de emergencia deberán estar suficientemente detallados y validados, garantizar la integridad permanente de los datos y no comprometer de ningún modo la ejecución del estudio. El personal que participa en los estudios, de conformidad con los Principios de BPL, deberá estar debidamente informado de todos estos planes de emergencia.

Los procedimientos de recuperación del procesamiento de un sistema informático dependerán siempre de la importancia del sistema, pero es indispensable conservar copias de salvaguardia de todos los software. Si los procedimientos de recuperación precisan una modificación del hardware o del software, podrá ser necesario validar de nuevo el sistema.

5. Datos

Los Principios de BPL definen los datos crudos como un conjunto de informes y documentos originales de laboratorio, e inclusive los datos incorporados directamente en un ordenador por mediación de un interfaz de instrumentación, que se derivan a su vez de las observaciones y de los trabajos originales llevados a cabo en el marco de un estudio y, que se precisan para la reconstitución y la evaluación del informe relativo a este estudio.

Los sistemas informáticos operados de conformidad con los Principios de BPL, pueden estar asociados a datos crudos de tipo sumamente diversos: así, puede tratarse de soportes de datos electrónicos, de salidas de ordenadores o de instrumentos, e incluso de microfilms/fichas. Los datos crudos se definirán para cada sistema informático.

Los sistemas informáticos utilizados para obtener la adquisición, el procesamiento, la comunicación o el archivado de los datos crudos estarán siempre proyectados para que exista la posibilidad de proceder a un análisis retrospectivo para que aparezcan todas las modificaciones de los datos sin ocultar los datos iniciales. También deberá ser posible asociar a cada modificación a la persona que ha procedido a ella, por medio de firmas (electrónicas) con incorporación de fecha y hora. Las modificaciones deberán estar justificadas en todos los casos.

Cuando los datos crudos se conservan por vía electrónica, será preciso garantizar las condiciones necesarias para la conservación a largo plazo del tipo de datos correspondientes, teniendo siempre en cuenta la duración útil de los sistemas informáticos. En caso de modificación de hardware y de software, deberá existir siempre la posibilidad de acceder y conservar los datos crudos sin correr el riesgo de comprometer su integridad.

Las informaciones auxiliares, y básicamente los registros de mantenimiento y los registros de calibración, necesarios para verificar la validez de los datos crudos o permitir la reconstitución de un proceso o de un estudio, deberán siempre archivarse debidamente.

Los procedimientos de operación de un sistema informático deberán también describir los procedimientos de adquisición de datos de sustitución que se han de utilizar en caso de fallo del sistema. En este caso, todos los datos crudos registrados manualmente y, acto seguido, adquiridos, deberán ser claramente señalados como tales y conservados A título de registros originales, los procedimientos manuales de salvaguardia podrán servir para reducir en todo lo posible los riesgos de pérdida de datos y tener la seguridad de que los registros de sustitución serán debidamente conservados.

Cuando, con motivo del envejecimiento de un sistema, se precisa transferir los datos crudos hacia otro sistema por vía electrónica, se utilizará un procedimiento debidamente seguro cuya integridad se habrá verificado previamente. Si no se puede proceder a esta transferencia, los datos crudos serán transferidos hacia otro soporte y se verificará la exactitud de la copia antes de destruir los archivos electrónicos originales.

6. Seguridad

Se deberán tener en cuenta procedimientos de seguridad suficientemente seguros para proteger el hardware, el software y los datos contra cualquier alteración, modificación no autorizada o pérdida. En este contexto, la seguridad abarca también la prevención del acceso no autorizado o las modificaciones del

sistema informático y de los datos contenidos en el sistema. También será conveniente tener en cuenta los riesgos de alteración de los datos por los virus u otros fenómenos. También se deberán tomar las medidas de seguridad necesarias para garantizar la integridad de los datos en caso de fallo del sistema a corto y largo plazo.

Seguridad física

Se deberán tener también en cuenta las medidas físicas de seguridad para limitar únicamente al personal autorizado el acceso a los equipos informáticos, a los equipos de comunicación, a los periféricos y a los soportes electrónicos. Al tratarse de los equipos que no se encuentran instalados en "salas informáticas" especializadas (PC y terminales, por ejemplo), será preciso tener en cuenta como mínimo, un control convencional para el acceso a las instalaciones de pruebas. No obstante, cuando estos equipos se encuentran situados a distancia (elementos portátiles o enlaces por módem) se deberán tomar otras medidas correspondientes al caso.

Seguridad lógica (software)

Para cada sistema o aplicaciones de carácter informático, se deberán tomar las medidas de seguridad lógica para impedir el acceso no autorizado a los sistemas, aplicaciones y datos informáticos. Es indispensable garantizar que únicamente se utilizan las versiones aprobadas y los softwares validados. La seguridad lógica puede presuponer una supervisión para tener la seguridad de que cada utilizador posee una identidad única acompañada de una contraseña. Cualquier introducción de datos o de softwares procedentes de fuentes externas deberá estar debidamente controlada. Estos controles se podrán obtener por medio del software operativo, por programas específicos de seguridad, programas integrados a las aplicaciones o por varios de estos medios en combinación.

Integridad de los datos

Habida cuenta de que el mantenimiento de la integridad de los datos constituye uno de los objetivos preliminares de los Principios de BPL, es preciso que cualquier persona involucrada en un sistema informático sepa que es indispensable tener en cuenta las diversas consideraciones que se acaban de mencionar en materia de seguridad. La Dirección deberá tener la seguridad de que el personal es perfectamente consciente de la importancia de la seguridad de los datos y que conoce los procedimientos y funciones del sistema que permiten garantizar una correcta seguridad, así como las consecuencias de cualquier defecto de seguridad. Estas funciones podrán corresponder a una vigilancia de rutina del acceso al sistema, la aplicación de programas de verificación de los archivos y la notificación de anomalías y/o tendencias.

Salvaguardia

En la práctica, cuando se utilizan sistemas informáticos, se procede a hacer copias de salvaguardia de todos los softwares y datos para poder reiniciar el sistema tras un fallo susceptible de comprometer su integridad (deterioro del disco duro, por ejemplo). Por consiguiente, la copia de salvaguardia debe poder constituir una fuente de datos crudos que serán procesados como tales.

7. Validación de los sistemas informáticos

Los sistemas informáticos deberán estar adaptados a las tareas para las cuales están destinados. Será conveniente tener debidamente en cuenta los siguientes aspectos:

Recepción

Los sistemas informáticos deben estar proyectados de conformidad con los Principios de BPL y su introducción se deberá planificar previamente en todos los casos. Una documentación adecuada debe demostrar que cada sistema se ha desarrollado bajo control y, de preferencia, de conformidad con las normas de calidad y con las normas técnicas reconocidas (ISO 9001, por ejemplo). Además, parece importante disponer de elementos concretos que demuestren que la conformidad del sistema con los criterios de recepción por la instalación de pruebas se ha verificado antes de su puesta en servicio. Las pruebas oficiales de recepción exigen proceder a ensayos según un plan previamente determinado y conservar los documentos relativos a todos los procedimientos de pruebas, los datos de ensayo, sus resultados, un resumen preciso de estas pruebas y un documento de recepción oficial.

En el caso de sistemas suministrados por un vendedor, una gran parte de la documentación creada durante el transcurso del desarrollo permanecerá en ciertos casos en el domicilio del vendedor. En tal caso, se deberá conservar en la instalación de pruebas un dossier relativo a la evaluación y/o la verificación oficial por el vendedor.

Evaluación retrospectiva

Para ciertos sistemas, puede ocurrir que el imperativo de conformidad con los Principios de BPL no haya sido ni previsto ni especificado. En tal caso, será conveniente disponer de elementos que permitan justificar la utilización de estos sistemas; básicamente, se tratará de una evaluación retrospectiva para valorar su adecuación.

Una evaluación retrospectiva da comienzo por la colecta de todas las informaciones retrospectivas relativas al sistema informático. Estos registros son examinados y un resumen escrito será preparado. Este resumen de evaluación retrospectiva deberá indicar los elementos disponibles que vienen en apoyo de una validación y cómo es preciso proceder en el futuro para que el sistema informático sea validado.

Verificación de las modificaciones

La verificación de las modificaciones constituye la aprobación y la justificación oficiales, documentos de apoyo, de cualquier modificación del sistema informático durante su duración operativa. La verificación de las modificaciones será necesaria cuando una modificación corre el riesgo de afectar la validez del sistema informático. Los procedimientos de verificación de las modificaciones deberán ser efectivos a partir del momento en que el sistema pasa a ser operativo.

El procedimiento deberá describir el método de evaluación para determinar en qué medida serán necesarios los nuevos controles para confirmar la validez del sistema. Los procedimientos de verificación de las modificaciones deberán precisar el nombre de las personas responsables de determinar si una verificación de las modificaciones es necesaria y, en caso afirmativo, aprobarla.

Sea cual fuere el origen de la modificación (proveedor o desarrollo interno), una información adecuada deberá ser facilitada en el marco del proceso de verificación de las modificaciones. Los procedimientos de verificación deberán garantizar la integridad de los datos.

Mecanismo auxiliar

Para tener la seguridad de que un sistema informático sigue estando adaptado a las tareas para las cuales están destinado, se deberán tener en cuenta mecanismos auxiliares para garantizar el correcto funcionamiento y el uso correcto del sistema. Podrá tratarse de disposiciones relativas a la gestión del sistema, la capacitación, el mantenimiento, la asistencia técnica, la auditoría y/o la evaluación de los resultados obtenidos. La evaluación de los resultados obtenidos consiste en un examen oficial efectuado periódicamente, con objeto de verificar que el sistema sigue respondiendo siempre a los criterios de resultados prácticos, en términos, básicamente de fiabilidad, de sensibilidad y de capacidad.

8. Documentación

Los elementos que figuran enumerados a continuación tienen por objeto describir, a título informativo, la documentación mínima necesaria para el desarrollo, la validación, la operación y el mantenimiento de los sistemas informáticos.

Instrucciones

Deberán existir instrucciones escritas de la Dirección que incluyan, básicamente, la adquisición, las características, el concepto, la validación, la experimentación, la instalación, la operación, el mantenimiento, el personal responsable, el control, la auditoría, la verificación y la puesta fuera de servicio de los sistemas informáticos.

Descripción de las aplicaciones

Para cada aplicación, se deberá disponer de una documentación completa relativa a:

- La denominación del software de aplicación o el código de identificación, así como una descripción clara y detallada de la vocación de la aplicación.

- El hardware (con los números de los modelos) sobre el cual se opera el software de aplicación.

- El sistema operativo y los demás softwares (herramientas, por ejemplo) utilizados en relación con la aplicación.

- El (o los) lenguaje(s) de programación de la aplicación y/o las herramientas de bases de datos que se utilizan.

- Las principales funciones llevadas a cabo por la aplicación.

- Una descripción general de los tipos y flujos de datos del concepto de las bases de datos asociadas a la aplicación.

- Las estructuras de los archivos, los mensajes de errores y de alarma y los algoritmos asociados a la aplicación.

- Los módulos del software de aplicación con los números de sus versiones.

- La configuración y los interfaces entre los módulos de aplicación y hacia los equipos y otros sistemas.

Programa fuente

Algunos países de la OCDE requieren que el programa fuente del software de aplicación se encuentre disponible, o pueda ser obtenido, en la instalación de pruebas.

Procedimientos normalizados de operación

Una gran parte de la documentación relativa a la utilización de los sistemas informáticos, se habrá de presentar en forma de Procedimientos normalizados de operación. Entre otros deberán incluir:

- Los procedimientos relativos a la operación de los sistemas informáticos (hardware/software) y las responsabilidades del personal interesado.

- Los procedimientos relativos a las medidas de seguridad utilizadas para detectar y precaverse contra los accesos no autorizados y las modificaciones de los programas.

- Los procedimientos y autorizaciones relativas a las modificaciones de los programas y registros de las modificaciones.

- Los procedimientos y autorizaciones relativas a las modificaciones de los equipos (hardware/software), e inclusive, llegado el caso, las pruebas antes de empleo.

- Los procedimientos relativos a las pruebas periódicas para verificar el funcionamiento de la totalidad del sistema o de ciertos elementos, y el registro de estas pruebas.

- Los procedimientos relativos al mantenimiento de los sistemas informáticos y de cualquier otro equipo auxiliar.

- Los procedimientos relativos al desarrollo de softwares y los ensayos de recepción, así como el registro de todos los ensayos de recepción.

- Los procedimientos de salvaguardia para todos los datos almacenados y los planes de emergencia en caso de producirse fallos.

- Los procedimientos relativos al archivado y la extracción de todos los documentos, softwares y datos informáticos.

- Los procedimientos relativos al control y la verificación de los sistemas informáticos.

9. Archivado

Los Principios de BPL relativos al archivado de los datos se deberán aplicar sistemáticamente para todos los tipos de datos. Por consiguiente, es de suma importancia que los datos informáticos se encuentren almacenados con los mismos niveles de control de acceso, de indización y de facilidad de extracción que los demás tipos de datos.

Cuando los datos electrónicos de más de dos estudios se almacenan en un único soporte (disco o cinta), se deberá tener en cuenta un índice detallado.

También podrá ser necesario dotar a ciertas instalaciones de dispositivos de protección del sitio, para garantizar la integridad de los datos informáticos almacenados. Si para ello se precisan instalaciones suplementarias de archivado, la Dirección tratará de definir correctamente el personal responsable de la gestión de los archivos y limitar su acceso únicamente al personal autorizado. También será preciso implementar procedimientos que garanticen la integridad a largo plazo de los datos almacenados por vía electrónica. Si el acceso a los datos a largo plazo parece plantear problemas o si se ha tenido en cuenta poner a ciertos sistemas informáticos fuera de servicio, se establecerán los procedimientos adecuados para garantizar que los datos siguen siendo legibles. Por ejemplo, podrá tratarse de preparar las salidas sobre soporte de papel o transferir los datos hacia otro sistema.

Ningún dato almacenado por vía electrónica se podrá destruir sin la previa autorización de la dirección y sin aplicación de la documentación adecuada. Los demás datos auxiliares relativos a los sistemas informáticos, como por ejemplo los programas fuente y los archivos de desarrollo, de validación, de operación, de mantenimiento y de control se deberán conservar durante, como mínimo el mismo lapso de tiempo que los registros y los estudios asociados a estos sistemas.

DEFINICIÓN DE LOS TÉRMINOS[1]

Control de las modificaciones: Evaluación permanente tomando como fundamento los documentos justificantes de las operaciones ejecutadas por un sistema y de su modificación para determinar si es necesario aplicar un procedimiento de validación tras cualquier modificación del sistema informático.

Criterios de recepción: Criterios expresamente definidos que es conveniente respetar para concluir positivamente la fase de pruebas o de ensayos o considerar que el sistema responde a un pliego de condiciones.

Ensayo de recepción: Ensayo oficial de un sistema informático en el contexto operativo proyectado para verificar si todos los criterios de recepción de la instalación de pruebas se han respetado debidamente y si el sistema se puede aceptar para funcionar en modo operativo.

Software (Aplicación): Un programa incorporado o desarrollado, adaptado o personalizado en función de las condiciones de la instalación de pruebas, para garantizar los procedimientos de control, la colecta, el procesamiento, la presentación y/o archivado de los datos.

Software (sistema operativo): Programa o conjunto de programas o de subprogramas que gobierna el funcionamiento del ordenador. Un sistema operativo puede llevar a cabo las tareas como la asignación de recursos, la planificación, la gestión de las entradas/salidas y la gestión de los datos.

Hardware: Conjunto de elementos físicos de un sistema informático que incluye la unidad central del ordenador y sus periféricos.

Normas técnicas reconocidas: Normas promulgadas por los organismos nacionales o internacionales de normalización (ISO, IEEE, ANSI, etc.).

Periférico: Cualquier equipo conectado con un sistema o elemento auxiliar o a distancia, como por ejemplo, las impresoras, módems, terminales, etc.

Programa fuente: Programa informático original redactado en un lenguaje legible por el hombre (lenguaje de programación) que se traduce, acto seguido, en lenguaje de máquina antes de poder ser ejecutado por el ordenador.

Salvaguardia: Disposiciones proyectadas para recuperar los archivos de datos o softwares, iniciar de nuevo el procesamiento o utilizar los equipos informáticos de sustitución en caso de fallo del sistema o de siniestro.

---

[1] Existen otros términos que figuran definidos en "Los Principios de la OCDE de Buenas Prácticas de Laboratorio".

Seguridad: Protección del hardware y del software contra el acceso, la utilización, la modificación, la destrucción o la divulgación ya sean accidentales o delictivos. La seguridad atañe también al personal, los datos, las comunicaciones y la protección física y lógica de las instalaciones informáticas.

Firma electrónica: La entrada, en forma de impulsos magnéticos o de datos informáticos adquiridos, de cualquier símbolo o conjunto de símbolos, ejecutada, adaptada o autorizada por una persona para representar su firma manuscrita.

Sistema informático: Grupo de elementos del equipo (hardware), acompañado de los softwares correspondientes, proyectado y ensamblado para permitir una función o un grupo de funciones determinadas.

Validación de un sistema informático: Operación que permite demostrar que un sistema informático corresponde perfectamente a las tareas para las cuales está destinado.