Auditoría Plan de Validaciones CSV

plan de migración y auditoría validaciones sistemas de laboratorios y Excel

➢ Programa: Certifícate como Auditor Interno GMP

Derechos de Autor y Propiedad Intelectual

Para permisos, consultas o más información, por favor contacte con nuestro departamento legal a través de legal@cercalgroup.com.

Introducción

La Validación de Sistemas Informáticos (CSV) es crucial en la industria farmacéutica para asegurar que los sistemas utilizados en fabricación y control de calidad cumplan con los estándares de integridad de datos y seguridad. En un entorno donde la precisión y la confiabilidad son esenciales, la CSV garantiza que los sistemas sean consistentes y operen según lo previsto, siguiendo normativas como PE-009 Annex 11, ISPE GAMP 5, EUDRALEX 4 Annex 11, y CFR 21 Part 11. Estas directrices, enfatizadas por la FDA desde 1983, aseguran la conformidad regulatoria y protegen tanto a consumidores como a empresas de riesgos asociados con sistemas no validados.

Este libro explora en profundidad los principios, metodologías y mejores prácticas para la validación de sistemas informáticos en la industria farmacéutica. Aborda los desafíos comunes en la validación, estrategias efectivas para la migración de datos, optimización de herramientas como Excel en entornos regulados, y el rol esencial del auditor. Además, destaca la importancia de la criticidad en la validación y ofrece un enfoque integral para diseñar un plan de auditoría eficaz. Esta guía práctica es esencial para profesionales que buscan asegurar la integridad, seguridad y conformidad de sus sistemas informáticos.

La **validación de Sistemas Informáticos (CSV)** se ha convertido en un componente esencial dentro de la industria farmacéutica, asegurando que los sistemas informáticos utilizados en la fabricación, control de calidad, y procesos regulados cumplan con los estándares de integridad de datos y seguridad. Este enfoque sistemático hacia la CSV está regido por un conjunto de normativas y guías regulatorias, incluyendo el **PE-009 Annex 11, ISPE GAMP 5, EUDRALEX 4 Annex 11, y CFR 21 Part 11.**

Estas referencias establecen los requisitos fundamentales para la validación de sistemas informáticos, asegurando que sean consistentes, fiables y capaces de operar de acuerdo con los propósitos previstos. La importancia de adherirse a estas directrices fue subrayada por la FDA en 1983 a través de su publicación conocida como 'bluebook', que marcó un hito al enfatizar la necesidad de establecer procesos de validación rigurosos para los sistemas informáticos en el sector farmacéutico.

Este enfoque no solo mejora la confiabilidad y seguridad de los datos generados por estos sistemas, sino que también garantiza la conformidad con los estándares regulatorios, protegiendo así tanto a los consumidores como a las empresas de los riesgos asociados con sistemas no validados o insuficientemente seguros.

La Esencia de la Validación de Sistemas Informáticos

Comprendiendo la Validación de Sistemas Informáticos

La validación de sistemas informáticos representa un pilar crucial en la infraestructura tecnológica de cualquier industria sujeta a regulación, especialmente en el sector farmacéutico. Este proceso no solo asegura que los sistemas informáticos cumplan con los requerimientos específicos para su uso previsto, sino que también verifica que dichos sistemas sean capaces de mantener su fiabilidad a lo largo del tiempo.

Definición y Propósito

La **validación de un sistema informático** se define como la confirmación, a través de un examen meticuloso y la provisión de evidencia objetiva, de que las especificaciones de un software están alineadas con las necesidades y expectativas del usuario final. Además, esta validación garantiza que todos los requisitos particulares, implementados mediante el software, pueden ser satisfechos de manera constante y fiable.

Normativas y Guías Regulatorias

Este concepto se fundamenta en los **"Principios generales de validación de software: guía final para la industria y el personal de la FDA".** Estos principios no solamente establecen el marco para una validación efectiva, sino que también subrayan la importancia de la evidencia objetiva como base para confirmar la adecuación y fiabilidad del software utilizado en entornos regulados.

Implicaciones Prácticas

En la práctica, la validación de sistemas informáticos abarca desde la fase inicial de diseño del software hasta su implementación final, incluyendo pruebas rigurosas y documentación exhaustiva que respalde cada etapa del proceso.

Este enfoque asegura no sólo la conformidad con los estándares regulatorios, sino también la optimización de la eficiencia operativa y la mitigación de riesgos asociados con el manejo de datos críticos.

La validación de sistemas informáticos es un requisito indispensable para garantizar que los procesos tecnológicos dentro de las industrias reguladas sean seguros, fiables y conformes a las expectativas regulatorias.

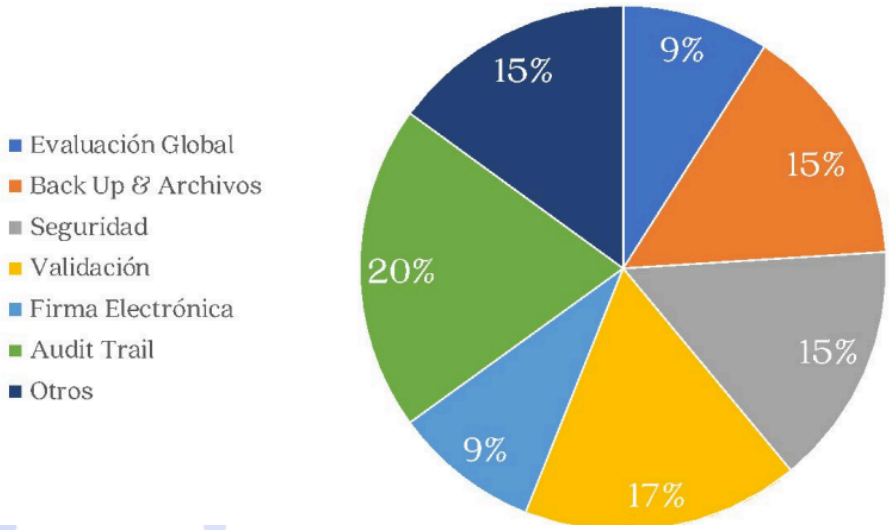
Al adherirse a las guías y principios establecidos por entidades como la FDA, las organizaciones pueden asegurar que sus sistemas informáticos cumplan de manera consistente con los requisitos específicos, fortaleciendo así la integridad de sus operaciones y la confianza en sus resultados.

Desafíos Comunes en la Validación de Sistemas Informáticos: Una Perspectiva de Auditoría

Análisis de Hallazgos en Auditorías de Validación de Sistemas Informáticos

La validación de sistemas informáticos en entornos regulados, especialmente en sistemas de planificación de recursos empresariales (ERP), es fundamental para asegurar la integridad de los datos y el cumplimiento normativo.

A lo largo de diversas auditorías, se han identificado patrones de deficiencias que resaltan la importancia de un enfoque sistemático y riguroso en la validación de sistemas informáticos (CSV). Este capítulo explora los hallazgos más comunes en auditorías de CSV, ofreciendo una guía para abordar estos desafíos de manera efectiva.



Evaluación Global

Los errores más frecuentes en la evaluación global de **sistemas ERP** destacan:

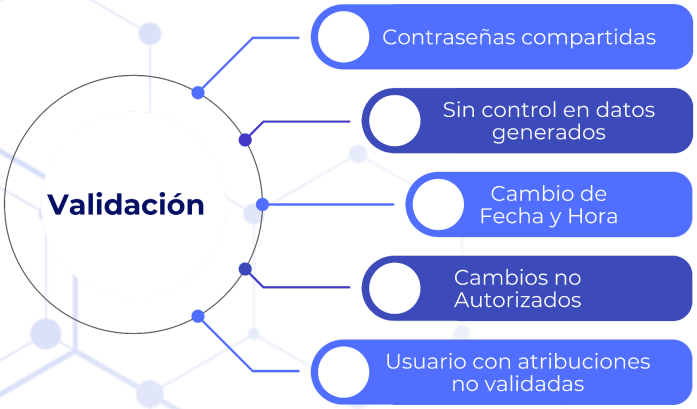
1. Ausencia de una visión detallada del sistema: Falta de comprensión profunda sobre la funcionalidad y el alcance del sistema.
2. Ignorancia de un enfoque basado en el riesgo: Falta de aplicación de principios de gestión de riesgos para priorizar y guiar el proceso de validación.

3. Selección de proveedores inadecuados: Elección de proveedores que no cumplen con los requisitos de calidad y seguridad necesarios.
4. Deficiencias en procesos clave: Omisión en la implementación de procesos esenciales para la operación y el mantenimiento del sistema.
5. Falta de calificación de infraestructura: Inadecuada verificación y validación de la infraestructura tecnológica soportante.

Validación

Dentro del ámbito de la validación, se han observado las siguientes problemáticas:

- Uso de contraseñas compartidas que comprometen la seguridad.
- Carencia de control sobre los datos generados, exponiendo a riesgos de integridad de datos.
- Modificaciones no autorizadas y cambios en fechas y horas que pueden afectar el registro y trazabilidad de las operaciones.
- Usuarios con atribuciones no validadas, lo que podría resultar en accesos indebidos o manipulación de datos.



Transacciones

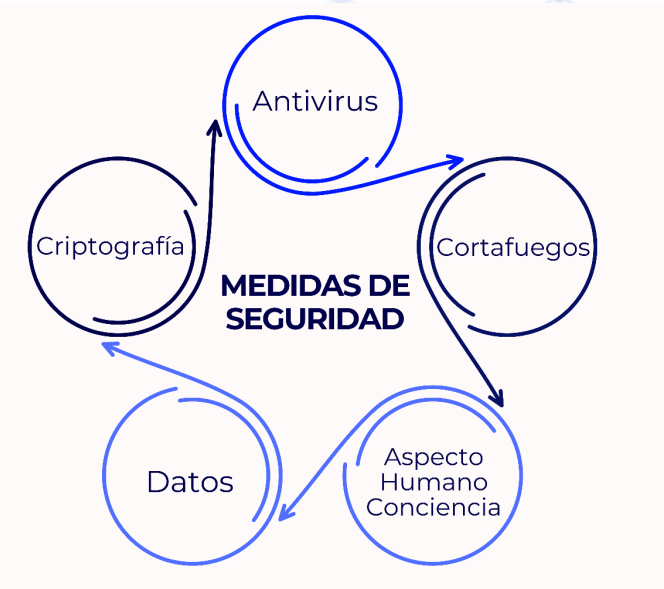
Los aspectos críticos en la gestión de transacciones incluyen:

- Ausencia de rastreo de auditoría (Audit Trail), esencial para la reconstrucción de eventos.
- Fallos en identificar usuarios y contraseñas, comprometiendo la autenticidad de las acciones realizadas en el sistema.
- Procesos de aprobación, habilitación o liberación no autorizados, que ponen en riesgo la validez de los datos y procesos.
- Eliminación de datos y transacciones sin controles adecuados, afectando la integridad y la disponibilidad de los registros.

Seguridad

La seguridad de los sistemas informáticos abarca:

- Implementación de criptografía y antivirus, junto con cortafuegos, para proteger contra amenazas externas e internas.
- Fomento de una cultura de conciencia sobre seguridad entre el personal, vital para la protección de la información.



Consideraciones Adicionales

La adopción de un **Audit Trail** estándar, el uso correcto de firmas digitales y la gestión de claves y contraseñas son aspectos fundamentales para asegurar la validación efectiva del sistema. Además, es crucial mantener un registro detallado y controlado de todas las transacciones, ya sean aprobadas, en cuarentena o rechazadas, y asegurar la precisión en el registro de fechas y horas.

Los hallazgos en auditorías de CSV en sistemas ERP revelan la necesidad imperativa de un enfoque detallado y basado en riesgos para la validación de sistemas informáticos. Al abordar proactivamente estas áreas comunes de deficiencia, las organizaciones pueden mejorar significativamente la seguridad, la eficiencia y el cumplimiento normativo de sus sistemas informáticos.

Estrategias Efectivas para la Migración de Datos en Sistemas Informáticos

Planificación y Ejecución de una Migración de Datos Segura y Eficiente

La migración de datos es un componente crítico en la gestión de sistemas informáticos, especialmente en entornos que demandan alta precisión y seguridad, como en la industria farmacéutica. Esta tarea, aunque necesaria para la actualización y mejora de sistemas, conlleva sus propios riesgos y desafíos.

A continuación, se detallan las prácticas recomendadas para una migración de datos eficaz, dividida en migraciones manuales y automáticas, seguida de consideraciones esenciales antes de iniciar este proceso.

Tipos de Migración de Datos

- Migración Manual: Implica la carga de datos al sistema de manera manual, utilizando formularios como hojas de Excel, Access, entre otros, o ingresándolos directamente en el sistema. Aunque flexible, este método es inherentemente riesgoso debido a la posibilidad de error humano, siendo crítico para datos maestros como cantidad, fecha, hora, estado, identificación y código de producto.
- Migración Automática: Se realiza mediante el uso de herramientas de transferencia de datos, cargas masivas de bases de datos o restauraciones de backup. Este método minimiza el riesgo de error humano, aunque requiere una vigilancia especial durante la restauración de backups para asegurar la integridad de los datos.

Consideraciones Previas a la Migración de Datos

Antes de proceder con la migración de datos, es fundamental:

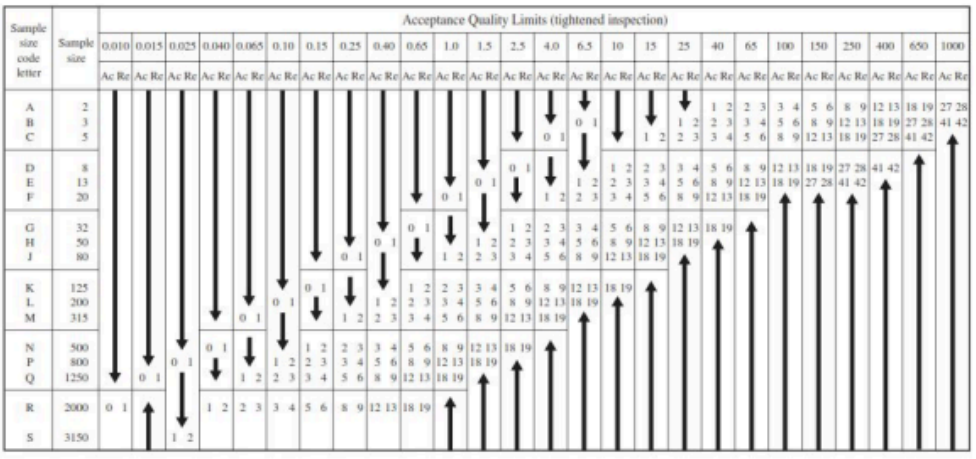
1. Elaborar un Plan de Trabajo: Definir las personas involucradas, sus roles, responsabilidades y actividades.
2. Análisis de Riesgos: Identificar posibles fallos y desarrollar estrategias de mitigación.
3. Permisología: Asegurar que todos los participantes cuenten con los permisos adecuados según su experiencia y conocimiento.
4. Capacitación: Entrenar al personal involucrado en las tareas y responsabilidades que enfrentarán.
5. Lista de Productos: Identificar los productos que serán afectados por la migración.
6. Auditoría: Mantener una pista de auditoría de los sistemas para documentar el proceso de migración.
7. Principios ALCOA y ALCOA+: Garantizar la completitud, disponibilidad, contemporaneidad y atribución de los datos.
8. Originalidad: Asegurar la autenticidad de los datos a migrar.
9. Precisión: Verificar la exactitud de los datos, incluyendo cantidades y especificaciones.
10. Integridad de Datos: Confirmar que los datos migrados estén completos mediante el análisis del tamaño de archivos y muestreos de inspección.

11. Documentación: Registrar todos los ensayos y desviaciones ocurridas durante la migración.
12. Normativa ANSI/ASQ Z1.4-2003: Aplicar métodos de muestreo de datos basados en procedimientos y tablas estandarizadas para la inspección por atributos.

Una migración de datos bien planificada y ejecutada es vital para la integridad y seguridad de los sistemas informáticos en entornos regulados.

Siguiendo estas pautas, las organizaciones pueden minimizar los riesgos asociados con la migración de datos, asegurando la fiabilidad y eficiencia de sus sistemas.

Lot or batch size	Special inspection levels				General inspection levels		
	S-1	S-2	S-3	S-4	I	II	III
2 to 8	A	A	A	A	A	A	B
9 to 15	A	A	A	A	A	B	C
16 to 25	A	A	B	B	B	C	D
26 to 50	A	B	B	C	C	D	E
51 to 90	B	B	C	C	C	E	F
91 to 150	B	B	C	D	D	F	G
151 to 280	B	C	D	E	E	G	H
281 to 500	B	C	D	E	F	H	J
501 to 1200	C	C	E	F	G	J	K
1201 to 3200	C	D	E	G	H	K	L
3201 to 10000	C	D	F	G	J	L	M
10001 to 35000	C	D	F	H	K	M	N
35001 to 150000	D	E	G	J	L	N	P
150001 to 500000	D	E	G	J	M	P	Q
500001 and over	D	E	H	K	N	Q	R



Optimización y Seguridad en el Uso de Planillas de Excel para Entornos Regulados

Diseño y Estructuración Efectiva de Planillas de Excel

Las **planillas de Excel** son herramientas fundamentales en la gestión de datos en diversos ámbitos profesionales, incluidos los entornos altamente regulados. La correcta estructuración y configuración de estas planillas no solo facilita el análisis y la visualización de datos sino que también asegura su integridad y confidencialidad.

A continuación, se detallan aspectos clave para la optimización de planillas de Excel, desde su diseño hasta la implementación de medidas de seguridad.

Aspectos Clave en el Diseño de Planillas de Excel:

1. Estructuración de la Información: Es vital contemplar espacios adecuados para la información a mostrar y solicitar, incluyendo espacios destinados a gráficas.
2. Configuración Visual: Ajustar las márgenes de las hojas, definir la información para el encabezado y pie de página, y seleccionar un tamaño de hoja apropiado son pasos esenciales para una presentación clara y profesional.
3. Uniformidad y Estética: La elección del tipo, color y tamaño de fuente debe alinearse con la identidad corporativa, usando colores que faciliten la lectura y eviten la saturación visual. Es importante ocultar hojas o columnas irrelevantes para el usuario, minimizando la confusión.

Preparación para la Seguridad de la Información:

Antes de aplicar capas de seguridad, la hoja de cálculo debe estar completamente diseñada y programada de acuerdo con las necesidades específicas para las que fue creada. Esto incluye:

- Intuitividad para el Usuario: Las planillas deben ser accesibles y comprensibles, con medidas de seguridad activas que no obstaculicen la usabilidad.
- Manejo de Datos Críticos: Todas las fórmulas y celdas de entrada de datos deben tratarse como elementos críticos, dada su influencia directa en los resultados finales.

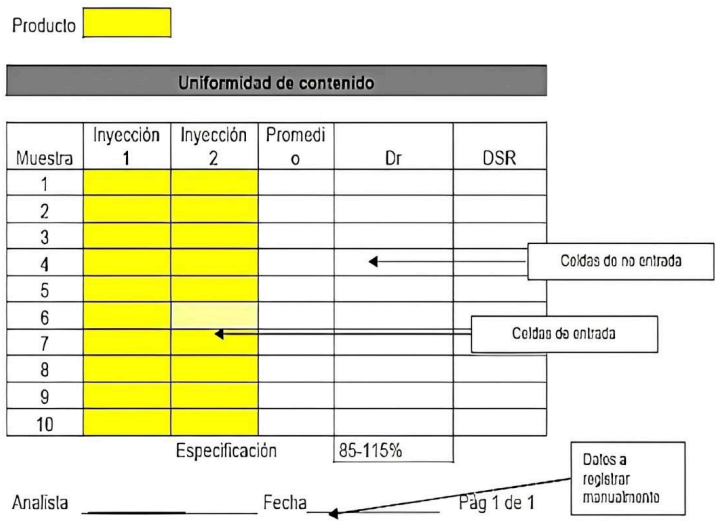
Implementación de Seguridades en Planillas de Excel:

Para garantizar la protección de la información, se deben considerar los siguientes aspectos:

- Entrada de Datos: Utilizar celdas sombreadas para indicar dónde debe ingresar información el usuario, marcando con N/A las celdas no requeridas.
- Impresión y Firma: Tras ingresar los datos, la impresión de la hoja debe incluir la dirección del directorio controlado donde se almacenan oficialmente, firmándose y fechándose manualmente las copias impresas.
- Almacenamiento de Claves de Acceso: Las claves implementadas para la seguridad de la planilla deben ser almacenadas por personal autorizado y no directamente involucrado en su uso rutinario.
- Control de Acceso: Las planillas deben alojarse en un directorio con permisos de solo lectura, claramente identificado y accesible solo para personal autorizado, con detalles como el nombre del documento, versión y autor claramente especificados en las propiedades del archivo.

La adecuada configuración y gestión de seguridad en planillas de Excel es crucial para asegurar la confidencialidad, integridad y disponibilidad de la información en entornos regulados.

Siguiendo estas prácticas recomendadas, las organizaciones pueden aprovechar al máximo las capacidades de Excel, manteniendo al mismo tiempo altos estándares de protección de datos.



El Rol Esencial del Auditor en la Validación de Sistemas Computarizados (CSV)

Características y Preparativos de un Auditor CSV Competente

La figura del auditor en el contexto de la Validación de Sistemas Computarizados (CSV) es fundamental para asegurar la conformidad y eficacia de los sistemas informáticos en entornos regulados, especialmente en la industria farmacéutica. Esta tarea exige un perfil profesional altamente calificado, capaz de navegar entre complejas regulaciones y estándares, y cuya labor es esencial para la integridad de los procesos y la seguridad del producto.

Perfil Ideal del Auditor CSV

- Conocimiento Especializado: La profundidad y amplitud del conocimiento en la industria farmacéutica son cruciales. Esto incluye una comprensión detallada de los procesos críticos como almacenamiento, calidad, manufactura y control de calidad.
- Dominio Regulatorio: Familiaridad con las normativas y guías de organismos como **ISPE, PIC/S, FDA y EMA**, que establecen los cimientos para las prácticas de CSV.
- Certificación Profesional: Poseer una certificación de auditoría, como la ISO 19011, es testimonio de su competencia y compromiso con la excelencia en el campo de auditoría.

Documentación y Preparativos Pre-Auditoría

Antes de emprender la auditoría, es vital que el auditor CSV esté debidamente preparado con una serie de documentos y autorizaciones esenciales, tales como:

1. Plan de Auditoría de CSV: Un documento detallado que establece el alcance, enfoque y cronograma de la auditoría.
2. Acuerdo de Confidencialidad: Para asegurar que toda información sensible manejada durante la auditoría se mantenga protegida.
3. Requisitos de Ingreso: Definir claramente las necesidades logísticas y de acceso para el equipo auditor.
4. Autorización del Auditado: Obtener una aceptación explícita del auditado para recibir al equipo de auditoría y colaborar en el proceso.

La efectividad de una auditoría CSV depende en gran medida del auditor, cuya experticia, conocimientos regulatorios y preparación son indispensables para identificar riesgos, validar la conformidad y garantizar la integridad de los sistemas computarizados.

La máxima "En Dios confiamos, todo los demás necesita documentación" refleja la necesidad imperante de una documentación exhaustiva y rigurosa, fundamentando cada hallazgo y recomendación en evidencia concreta.

De esta manera, el auditor CSV desempeña un rol crucial en el mantenimiento de estándares de calidad y seguridad en la industria farmacéutica, reforzando la confianza en los procesos y productos frente a reguladores y consumidores.

Diseñando un Plan de Auditoría Eficaz para CSV

Elementos Cruciales en la Documentación de Auditoría

Un plan de auditoría meticulosamente preparado es esencial para la validación efectiva de sistemas computarizados en entornos regulados, como la industria farmacéutica. Este plan debe abarcar todos los aspectos necesarios para asegurar que los sistemas no solo cumplen con los estándares establecidos, sino que también son capaces de mantener esa conformidad a lo largo del tiempo.

La documentación para la preparación de una auditoría debe incluir:

- Organigramas: Proporcionan una visión clara de la estructura organizacional y la distribución de responsabilidades.
- Registros de Entrenamiento: Verifican que el personal involucrado en el manejo de sistemas computarizados esté adecuadamente capacitado.
- Plan Maestro de Validación y Plan de Validación de Sistemas Computarizados: Estos planes son fundamentales para entender el enfoque y los métodos de validación empleados.
- Registros de Control de Cambios y de Problemas: Esenciales para evaluar cómo se gestionan los cambios y los desafíos en los sistemas.

- Requisitos del Sistema y Descripciones Generales: Ofrecen una comprensión detallada de lo que los sistemas están diseñados para hacer y cómo están configurados.
- Metodología de Desarrollo, Planes de Validación e Informes, y Registros de Pruebas: Estos documentos demuestran la rigurosidad del proceso de validación desde su planificación hasta su ejecución y revisión.

Objetivos Específicos del Plan de Auditoría

Para garantizar una auditoría exhaustiva y efectiva, el plan debe establecer objetivos claros en varias áreas clave, tales como:

- Sistema de Calidad: Asegurarse de que el personal de control de calidad revise y apruebe toda la documentación y procedimientos, y vigilar el cumplimiento de las Prácticas Operativas Estándar (POE).
- Instalaciones y Equipos: Evaluar la calificación de la infraestructura y el equipamiento, incluidas las computadoras, y verificar que los procesos de control de cambios estén bien establecidos y se sigan rigurosamente.
- Sistema de Materiales: Verificar la validación de los procesos informatizados relacionados con los materiales y asegurar la adherencia a los procesos de control de cambios.
- Sistema de Producción y Empaque y Etiquetado: Confirmar que los procesos de producción y empaque y etiquetado estén validados informatizadamente y que los procedimientos de control de cambios se cumplan de manera consistente.

El desarrollo de un plan de auditoría detallado y bien estructurado es un paso crítico hacia la validación efectiva de sistemas computarizados en la industria farmacéutica. Al asegurar una documentación exhaustiva y establecer objetivos claros para cada área de enfoque, las organizaciones pueden mejorar significativamente su capacidad para cumplir con las regulaciones vigentes, mantener la integridad de los datos y proteger la seguridad del paciente.

Este enfoque proactivo y organizado hacia la auditoría no solo facilita el cumplimiento normativo, sino que también impulsa la mejora continua de los sistemas y procesos.

La Importancia de la Criticidad en la Validación de Sistemas Computarizados

Entendiendo la Criticidad en el Contexto GxP

En el ámbito de las **Buenas Prácticas (GxP)** reguladas, la evaluación de la criticidad de los sistemas informáticos es un aspecto fundamental que no puede ser subestimado. Esta evaluación determina no solo la profundidad y el alcance de las auditorías y validaciones necesarias, sino también la intensidad de las medidas correctivas en caso de desviaciones.

Los inspectores, asumiendo una postura precautoria, tienden a considerar todos los componentes como críticos para GxP a menos que se presente una justificación sólida que demuestre lo contrario.

Evaluación de Riesgos y Clasificación de la Criticidad

La determinación de la criticidad de un sistema se basa en una evaluación meticulosa de riesgos que considera diversos factores, entre ellos:

- Naturaleza y Alcance de las Desviaciones: El impacto potencial de las desviaciones en los procesos críticos y su gestión es un factor determinante en la clasificación de la criticidad.
- Efecto sobre la Calidad del Producto y la Integridad de los Datos: Cualquier riesgo que pueda comprometer la calidad del producto o la veracidad de los datos se trata con suma importancia.
- Idoneidad y Oportunidad de las Medidas Correctivas: La capacidad de una organización para implementar acciones correctivas eficaces y oportunas es crucial para mitigar los riesgos identificados.
- Historial de Cumplimiento: Las autoridades regulatorias también consideran el historial de cumplimiento de una organización al evaluar la criticidad de sus sistemas.

Perspectiva Regulatoria sobre la Criticidad

Aunque la mayoría de las autoridades regulatorias adoptan un enfoque uniforme respecto a la criticidad, ciertas agencias como la **MHRA (Agencia Reguladora de Medicamentos y Productos Sanitarios del Reino Unido)** pueden mostrar cierta flexibilidad basada en la criticidad específica de un sistema dentro de las operaciones GxP.

Sin embargo, existen áreas donde la falta de diligencia puede resultar en problemas significativos, tales como:

- Descripción Detallada y Actualizada de los Sistemas Informáticos: La ausencia de documentación detallada que describa las funciones, seguridad e interacciones de un sistema es una bandera roja para los inspectores.
- Evidencia de Aseguramiento de la Calidad del Software y su Validación: La falta de evidencia sólida que respalde la calidad y la adecuada validación de los sistemas informáticos relacionados con GxP es considerada una desviación crítica.

La evaluación de la criticidad es un proceso esencial en la gestión de sistemas informáticos en entornos regulados por GxP.

Entender y aplicar correctamente estos principios permite a las organizaciones priorizar sus esfuerzos de validación y aseguramiento de la calidad, garantizando así la conformidad regulatoria y, lo más importante, la seguridad y eficacia de los productos destinados al consumo humano.

Objetivos Centrales en la Auditoría de Validación de Sistemas Informáticos

Fundamentos de la Inspección en Entornos Regulados

La auditoría de validación de sistemas informáticos juega un rol crítico en asegurar la integridad, seguridad, y conformidad regulatoria de las operaciones dentro de la industria farmacéutica y otros entornos regulados.

Estas auditorías se diseñan para evaluar exhaustivamente tanto la infraestructura tecnológica como los procesos de gestión de calidad, abordando múltiples aspectos críticos. A continuación, se detallan los objetivos principales de dichas auditorías, esenciales para comprender su alcance y finalidad.

Evaluación del Sistema de Gestión de Calidad y Desarrollo del Sistema

Las auditorías buscan verificar la adecuación y eficacia del sistema de gestión de calidad, incluyendo:

- Uso de Herramientas y Estándares: Confirmación de que las herramientas y estándares implementados son adecuados para los requisitos del sistema y las prácticas de la industria.
- Gestión de Proveedores: Evaluación de los roles y responsabilidades asignados a los proveedores, asegurando que sus contribuciones cumplan con los estándares de calidad y seguridad requeridos.

Validación de Sistemas Informáticos

Un foco principal de la auditoría es asegurar que los sistemas informáticos estén correctamente validados, lo cual incluye:

- Gestión de Documentación: Revisión de los procesos de control de documentos, desde su creación hasta su retiro, garantizando la trazabilidad y el control de cambios.
- Controles de Acceso: Verificación de los mecanismos de autenticación y autorización para asegurar la protección de los datos sensibles.
- Integridad de Datos: Evaluación de la captura, procesamiento, y almacenamiento de datos, incluyendo la transcripción contemporánea y la gestión de backups.

Gestión de la Seguridad de la Información

La auditoría también se extiende a la seguridad de la información, abarcando:

- Protección contra Malware: Confirmación de la existencia de medidas efectivas contra software malicioso, incluyendo antivirus y otros sistemas de detección.
- Seguridad de la Red: Revisión de la infraestructura de TI, incluidos cortafuegos y otras barreras de seguridad, para proteger contra accesos no autorizados y ataques cibernéticos.
- Registros Electrónicos y Pistas de Auditoría: Verificación de que los registros electrónicos sean precisos, íntegros, y auditable, con un control adecuado sobre las firmas electrónicas.

Fortalecimiento de la Infraestructura y Capacitación de Usuarios

Finalmente, la auditoría evalúa aspectos fundamentales como:

- Manejo de Comunicaciones: Examen de las transacciones e interacciones por correo electrónico, asegurando la seguridad y confidencialidad de la información compartida.
- Gestión de Configuraciones y Versiones: Verificación de que se mantenga un control estricto sobre las versiones del software y configuraciones del sistema.
- Programa de Entrenamiento: Revisión de los programas de capacitación para usuarios, enfocándose en promover una comprensión profunda del sistema y sus medidas de seguridad.

La auditoría de validación de sistemas informáticos es un proceso integral que abarca desde la evaluación de la gestión de calidad hasta la seguridad de la información, pasando por la validación del sistema en sí.

Su objetivo es no solo identificar áreas de mejora sino también garantizar el cumplimiento de las normativas vigentes, protegiendo así la calidad del producto y la seguridad del paciente.

Fundamentos de la Validación de Sistemas Computarizados (CSV)

Principios y Metodologías en la Validación de Software

La Validación de Sistemas Computarizados (CSV) es un proceso crítico en la industria regulada, especialmente en el sector farmacéutico, para asegurar que los sistemas informáticos cumplan con los requisitos específicos y funcionen de manera confiable.

Este proceso abarca desde el diseño inicial hasta la implementación final del software, enfocándose en la coherencia, integridad, y corrección tanto del software como de su documentación de soporte.

La Estrategia de "V" en CSV

Una herramienta esencial en el proceso de CSV es el **Diagrama en "V"**, que ilustra las etapas de validación en paralelo con las fases de desarrollo del software:

- Fase de Definición: Incluye la Especificación de Requisitos del Usuario (URS) y la Evaluación de Funciones Esenciales (EF), estableciendo las bases para el desarrollo.

- Análisis y Planificación: La identificación de riesgos y la planificación de transacciones y pruebas son cruciales para anticipar y mitigar posibles problemas.
- Ejecución y Revisión: La implementación de pruebas (IQ, OQ, PQ), el seguimiento de la trazabilidad, y la generación de reportes de validación aseguran que el software cumple con los requisitos especificados.
- Verificación de la coherencia: Se verifica la coherencia, completa y correcciones del software y su documentación de soporte, a través de pruebas formales y demostrables.

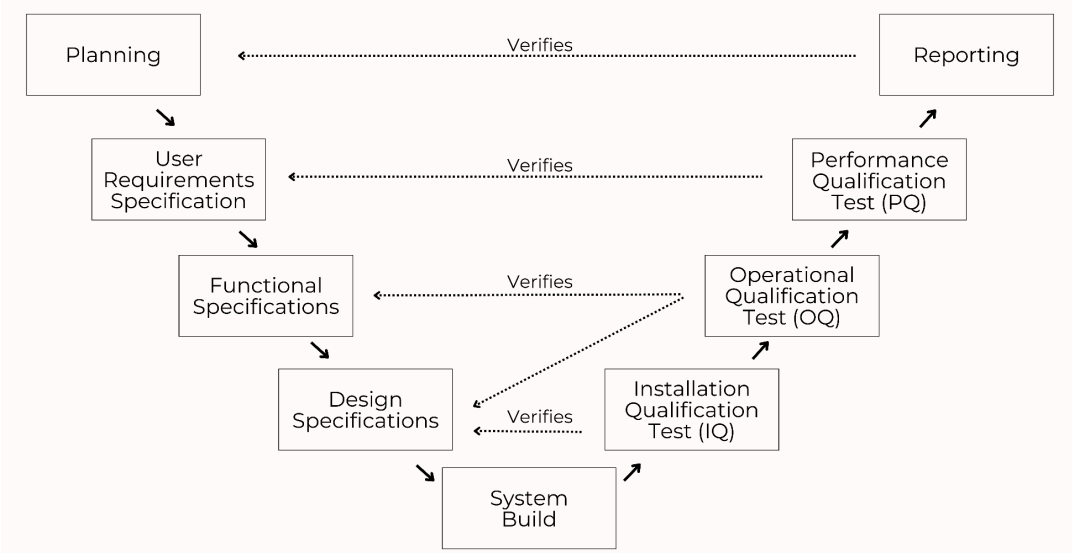
Aspectos Críticos en la Validación

Para lograr una validación efectiva, se deben considerar varios aspectos fundamentales:

- Confirmación por Examen: Es imperativo que el software se examine para confirmar que satisface las necesidades definidas de los usuarios y los usos previstos. Esto puede implicar revisiones de diseño, pruebas de código, y otros métodos de evaluación.
- Provisión de Evidencia Objetiva: La documentación detallada de las actividades de validación y los resultados de las pruebas es esencial para demostrar la validación del software.
- Necesidades del Usuario y Usos Previstos: El software debe ser examinado rigurosamente para asegurar que cumple con las expectativas del usuario, abarcando desde las funciones básicas hasta las aplicaciones más complejas.

La Validación de Sistemas Computarizados es un pilar en el aseguramiento de la calidad y la conformidad regulatoria de los sistemas informáticos en la industria farmacéutica y otros sectores regulados. El proceso de CSV, guiado por el Diagrama en "V" y centrado en una metodología rigurosa, garantiza que los sistemas informáticos sean fiables, seguros y efectivos para su propósito previsto.

Esta guía completa ofrece una base sólida para entender y aplicar los principios de CSV, asegurando que los profesionales estén equipados para enfrentar los desafíos de la validación de software en entornos regulados.


Planning
Verifies
Reporting
User Requirements Specification
Verifies
Performance Qualification Test (PQ)
Functional Specifications
Verifies
Operational Qualification Test (OQ)
Design Specifications
Verifies
Installation Qualification Test (IQ)
System Build

Resumen

La Validación de Sistemas Computarizados (CSV) es una piedra angular en el aseguramiento de la calidad y la conformidad regulatoria dentro de la industria farmacéutica y otros sectores regulados.

Este proceso meticuloso garantiza que los sistemas informáticos sean confiables, seguros y efectivos, cumpliendo con los rigurosos estándares establecidos por organismos como la FDA, EMA, entre otros. A través de la evaluación de la criticidad, la gestión de la seguridad, la adecuada migración de datos y el uso optimizado de herramientas como las planillas de Excel, se fortalece la integridad de los datos y la eficacia operativa.

El papel del **auditor CSV**, armado con un profundo conocimiento y un enfoque sistemático para la revisión y validación, es fundamental en este proceso, subrayando la importancia de una documentación exhaustiva y el cumplimiento de las normativas aplicables. En resumen, la CSV es un requisito indispensable para mantener los más altos estándares de calidad y seguridad en la era digital.