Requisitos de la información para la digitalización en el sector salud

Integridad de datos

Mayte Garrote
CTO de Oqotech

Las buenas prácticas en la gestión de la integridad de datos se componen de controles aportados por los sistemas informatizados, los equipos de proceso, los procedimientos implantados en la organización y de la verificación del comportamiento finalmente obtenido en los procesos afectados.

PALABRAS CLAVE: Data Integrity, Regla ALCOA+, Ciclo de vida de los datos, Flujo de información y gobierno de datos

Good practices in data integrity management are composed of controls provided by the computerized systems, the process equipment, the procedures implemented in the organization and the verification of the behavior finally obtained in the affected processes.

KEYWORDS: Data Integrity, ALCOA + Rule, Data life cycle, Information flow and data governance

INTRODUCCIÓN

La informatización de procesos de negocio críticos tiene cada día mayor peso entre las empresas del sector sanitario, farmacéutico, cosmético o alimentario. Los cambios tecnológicos que se están produciendo en los últimos años, con una demanda cada vez mayor de procesos digitalizados e información rigurosa en tiempo real, junto con la exigencia regulatoria, están convirtiendo la informatización de procesos y la validación de sistemas informatizados en acciones estratégicas y necesarias para cualquier compañía.

El uso de sistemas informatizados puede facilitar el acceso rápido a la información, y también puede ser una vía de reporte de datos por parte de agentes de la salud y los pacientes. Asimismo, los sistemas pueden ser utilizados como herramientas en la gestión de procesos industriales.

En este entorno es de vital importancia la integridad de los datos generados, procesados, representados o almacenados en estos sistemas. A lo largo del presente artículo vamos a identificar y detallar los requisitos aplicables a la gestión de la información en un contexto informatizado dentro del ámbito de sectores relacionados con la salud.

REQUISITOS DE LA REGLA ALCOA+

La principal expectativa regulatoria de cumplimiento de la integridad de datos se centraliza en la regla Alcoa+. Inicialmente cada letra de la palabra Alcoa representaba un requisito que debía cumplir la información; más tarde se ampliaron los requisitos añadiendo el símbolo + a la palabra Alcoa.

La integridad de datos se aplica a toda la información crítica de la organización y, por tanto, a todo el sistema de calidad. Estando dentro de

su alcance los documentos del sistema de calidad, sistemas informatizados y equipos de proceso. Lo que supone la estandarización en toda la organización, fijando criterios comunes e independientes del soporte formato o medio de los datos y su origen.

A continuación se analizan los requisitos de la regla Alcoa+. La aplicación de algunos requisitos va dirigida a los administradores de los sistemas informatizados, las características de los propios sistemas informatizados y/o a las verificaciones del comportamiento final del proceso. Por tanto, su aplicación tendrá tanto una parte técnica del sistema como procedimental.

ATRIBUIBLES

Los requisitos para los administradores del sistema son los siguientes:

- Gestión de usuarios. La codificación de los usuarios generados debe permitir identificar de forma única a la persona.
- Gestión de permisos de seguridad. Por puesto de trabajo, evitando el diseño de perfiles de seguridad por usuario. La definición de perfiles consiste en la asignación de accesos a funcionalidades a los usuarios capacitados.
- Control de acceso por usuario y bloqueo de cuentas tras varios intentos de acceso fallidos.
- Política de gestión de contraseñas. Definición de la complejidad, renovación y cambio periódico.

Los requisitos para los sistemas informatizados son los siguientes:

- En el registro de las tareas reguladas debe quedar identificada la persona o sistema que genera el dato.
- En el registro de las tareas reguladas debe quedar identificada la persona o sistema que realiza la actividad que genera o modifica datos.
- En el *audit trail* debe quedar registro del alta, baja o modificación de los usuarios, perfiles de seguridad y contraseñas.

LEGIBLES

Requisitos para sistemas:

- En el registro de las tareas reguladas debe quedar registro de los datos y metadatos necesarios.
- Se encontrarán disponibles tanto los datos originales como las modificaciones posteriores.
- En el registro de *audit trail* de las tareas reguladas debe quedar registro de los datos y metadatos necesarios: fecha/hora, usuario, entidad afectada, valor nuevo, valor antiguo y motivo de cambio (para modificaciones y bajas).

Siendo metadatos la información que describe los atributos del dato, proporcionando contexto y significado y sin los cuales el dato pierde valor y no podemos asegurar su integridad. Siendo *audit trail* el registro electrónico seguro que permite la reconstrucción de eventos relacionados con la creación, modificación o eliminación de registros electrónicos. Afecta a la configuración del sistema, a la propia gestión del proceso y a los registros generados.

SIMULTÁNEOS

Requisitos para sistemas:

- Registrado y visualizado en el momento en el que se realiza la actividad.
- Uso de fecha y hora administrada por la organización, sin opción de modificación para los usuarios finales.

Requisitos para usuarios:

- Registrado y visualizado en el momento en el que se realiza la actividad, sin el uso de soportes intermedios.
- Uso de fecha y hora administrada por la organización, en caso de que la fecha y hora se introduzca de manera manual. El registro de la fecha y hora del registro del dato se debe realizar siempre, independientemente de cuándo se obtuvo el dato.

Requisitos para desarrolladores y proveedores de servicios:

- En caso de que el proceso se componga de varias etapas, debe quedar registrado en cada una de las etapas el resultado parcial. En caso de error, no habrá pérdida de datos parciales.

ORIGINALES

El registro original puede ser descrito como la primera captura de información, ya sea grabada en papel o electrónicamente. Que preserva su contenido o significado y naturaleza.
Requisitos para usuarios:

- Registrado en el momento en el que se realiza la actividad directamente en los medios autorizados. Sin el uso de soportes intermedios no autorizados.
- Debe quedar registro de la primera lectura, medición o resultado calculado.
- En caso de que el usuario cometa un error en el registro del dato, el dato original y el modificado deben conservarse.
- Los usuarios no deben tener a su disposición copias no autorizadas de los documentos o formularios. Todos los documentos o formularios deben disponer de un identificador único.
- El diseño del formulario en papel debe disponer de espacio suficiente para correcciones. En caso de un registro electrónico, debe habilitarse la opción de modificación a usuarios autorizados, quedando registro del valor original y nuevo, así como el motivo del cambio, conforme se ha comentado en los requisitos del audit trail.
- Los revisores deben asegurarse de revisar los registros originales. En caso de datos dinámicos debe hacerse en los datos electrónicos.

EXACTOS

- Datos precisos que permitan la reconstrucción total de las actividades que han dado lugar a la generación de los mismos. La precisión del registro debe ser conforme a los datos obtenidos y a la precisión requerida para el proceso a gestionar.
- Formación para usuarios para el

registro de datos y uso de sistemas informatizados.

• Mantenimiento y calibración de equipos realizada conforme al procedimiento aprobados en el rango de medición apropiado.

COMPLETOS

• Se consideran datos completos a todos los datos y metadatos relevantes, incluida cualquier repetición o modificación.

• Cuando se generen múltiples resultados, el usuario debe asegurarse de que todos los resultados se registren correctamente.

• El usuario en el registro en papel o en el uso de sistemas informatizados debe seguir un procedimiento claramente definido para invalidar un registro. En ningún caso el registro original se destruirá, es más, se debe preservar como parte del dato completo.

• Los datos únicamente se pueden eliminar pasado el tiempo de archivo y siguiendo el procedimiento establecido.

CONSISTENTES

• De forma previa a la revisión de la conformidad de los datos críticos de acuerdo a las especificaciones técnicas, se debe evaluar la confiabilidad de los datos. Esto puede implicar revisión del *audit trail* y metadatos, verificar secuencias operativas o verificar datos originales.

PERDURABLES

• Los datos deben registrarse de forma permanente y mantenerse durante el periodo de retención declarado. Los procedimientos deben confirmar que los datos archivados, incluidos metadatos relevantes, estén disponibles y sean legibles por humanos.

• En caso de registros en papel, una vez completados los registros debe quedar establecido en un procedimiento la entrega a un responsable que gestione su almacenamiento seguro a lo largo del tiempo de archivo declarado.

• En caso de registros electrónicos, debe generarse una política de copias de seguridad que identifique las fuentes de datos, el lugar de origen del registro, el tipo de copias de seguridad y el destino de copias (evitando el almacenamiento de datos GxP en los equipos o PCs donde se originó el dato), así como determinar la periodicidad de la verificación de la correcta restauración de los datos.

DISPONIBLES

• Se debe asegurar que los datos GxP que se encuentren en periodo de archivo estén disponibles para el personal autorizado de la organización y las autoridades competentes.

• Debe comprobarse la accesibilidad y la legibilidad de los datos si se realizan cambios relevantes en el sistema (hardware o software); entonces la capacidad de recuperar los datos debe garantizarse y comprobarse.

CONOCIMIENTO COMPLETO DE LA ORGANIZACIÓN Y CONTROL BASADO EN EL RIESGO

El impacto de incidencias en los registro e integridad de datos puede ser muy significativo en industrias reguladas. Si afecta al producto, puede acarrear no conformidades y sanciones. Estas desviaciones pueden tener un impacto económico.

Aplicar controles basados en el riesgo es una estrategia necesaria teniendo en cuenta la afectación a la seguridad del paciente, calidad del producto e integridad de datos. Para el diseño de la gestión de riesgos (identificación, evaluación, gestión y seguimiento) es aconsejable tener en cuenta la metodología descrita por la ICH Q9.

Requisitos para la aplicación de la gestión de riegos:

• Conocimiento y comprensión completa de los procesos críticos de negocio.

• Identificando el alcance operativo de los sistemas informatizados presentes en la organización.

• Identificando el diseño de la infraestructura informática de la organización: centro de procesamiento de datos, seguridades físicas y lógicas, servidores, hardware y software, redes, comunicaciones y seguridades.

• Política de mantenimiento de los sistemas informatizados.

• Actividades subcontratadas. Conociendo el sistema de calidad de los proveedores de servicio tecnológicos, estableciendo acuerdos que determinen la actividad solicitada y auditándolos periódicamente para el seguimiento del cumplimiento de los acuerdos.

• Conocimiento y comprensión completa del flujo de información.

• Identificando los usuarios de la organización presentes en cada proceso, teniendo en cuenta su capacitación.

CONOCIMIENTO Y CONTROL DEL FLUJO DE INFORMACIÓN

La gestión de los datos debe ser considerado como un proceso en sí mismo; debe enfocarse a todo el ciclo de vida del dato. En la Figura 1 se identifican las principales fases del ciclo de vida del dato y los puntos críticos a monitorizar en cada una de ellas.

VERIFICACIÓN DE LOS CONTROLES APLICADOS Y MANTENIMIENTO DEL ESTADO DE CONTROL

Es necesario establecer mecanismos de verificación del comportamiento de gestión de la información finalmente obtenido en los procesos afectados, así como procedimientos para mantener el estado de control. A continuación se identifican las principales tareas de mantenimiento:

• Inventario de sistemas informatizados, equipos de proceso y flujos de información.

• Análisis de riesgos para establecer prioridades en la validación de sistemas informatizados.

• Validación de sistemas informatizados.

FIGURA 1. Puntos críticos en el ciclo de vida del dato

• Procedimientos de seguridad física y lógica.
• Gestión de usuarios, perfiles de seguridad y contraseñas.
• Plan de formación.
• Firmas electrónicas.
• Política de copias de seguridad y restauración de datos.
• Control y revisión del *audit trail*.
• Control de archivo de datos.
• Monitorización del rendimiento de equipos.
• Plan de contingencia y recuperación en caso de desastre.
• Plan de auditorías internas y a proveedores de servicio.

CONCLUSIONES

1. Nos encontramos en continuo aumento de la digitalización en el sector salud. Los sistemas informatizados se utilizan para aportar controles en tiempo real a los procesos críticos de las organizaciones, para el acceso a la información de forma más rápida y sencilla y como registro para pacientes y doctores.

2. Es de vital importancia el control y robustez de los datos generados, procesados, representados o almacenados en estos sistemas.

3. Existencia de la regla Alcoa+ como referente en la definición de requisitos para el cumplimiento de la integridad de datos.

4. Se requiere un conocimiento completo de los procesos de la organización para aportar los controles necesarios para el aseguramiento de la integridad de datos. Se debe establecer los controles basados en el riesgo. Los principales riesgos son los aportados por el proceso, tecnológicos y humanos.

5. Se requiere un conocimiento completo del flujo de información para controlar el origen de la información crítica, el procesamiento de los datos y el mantenimiento de los mismos.

6. Se requiere verificar de forma periódica el comportamiento de la gestión de la información finalmente obtenido en los procesos afectados, así como revisar de forma periódica las medidas de mitigación implantadas, como validaciones, cualificaciones y protocolos de gestión.

Bibliografía

[1] [4] ISPE, GAMP Good Practice Guide, "Records & Data Integrity". 2017.
[2] [4] ISPE, GAMP Good Practice Guide, "Data Integrity – Key Concepts". 2018.
[3] [1] ISPE, "GAMP5, "A Risk-Based Approach to Compliant GxP Computerized Systems". 2008.
[4] [19] WHO, "Annex 5, Guidance on Good Data and Record Management Practices". 2016
[5] [15] PIC/S, "Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments". 2016.
[6] [16] FDA, "Data Integrity and Compliance with cGMP. Guidance for Industry". 2016
[7] [17] MHRA, "GxP Data Integrity Guidance and Definitions". 2018
[8] [13] EMA/CHMP/ICH, "ICH guideline Q9 on quality risk management". 2015.
[9] [14] ISO, "ISO 27001, Sistemas de gestión de la seguridad de la información". 2014.