 

**Organización Internacional de Foro Internacional de**

**Normalización Acreditación**

3 enero 2016.

Orientación del Grupo de Prácticas de Auditoría ISO 9001 sobre:

**Sistemas de información documentada electrónica.**

1. Introducción

La creciente dependencia de las organizaciones de los medios electrónicos para la operación y el control de sus sistemas de gestión requiere que los organismos de certificación / registro y que sus auditores examinen nuevos enfoques para garantizar que las auditorías sean eficaces y eficientes. Deberán redefinir la forma en que se evalúan los procesos y la información documentada para verificar el cumplimiento con los criterios de auditoría.

Este documento se ha desarrollado para proporcionar pautas generales para la realización de auditorías de sistemas de gestión que son totalmente electrónicos o tienen un alto grado de información documentada en medios electrónicos. También proporciona directrices para que los organismos de certificación / registro y los auditores lo consideren como un complemento de las actividades normales de planificación y preparación que deben realizarse antes de una auditoría.

Este documento se centra en la auditoría de los requisitos de la norma ISO 9001, donde existe la posibilidad de utilizar medios electrónicos para obtener información documentada.

Este documento está dirigido a auditores de sistemas de gestión que tienen una amplia y variada gama de experiencia práctica con respecto al uso de medios electrónicos para la operación y el control de sistemas de gestión, es decir, sistemas de gestión que dependen de los medios electrónicos y las aplicaciones de software para su funcionamiento normal. Sin embargo, está escrito en un estilo que también permitirá que lo utilicen aquellos que solo tienen una experiencia limitada en computadoras y medios electrónicos.

Ya sea un organismo de certificación externo, un organismo de acreditación o una función de auditoría interna, la organización que lleva a cabo la auditoría ("la organización auditora") es responsable de garantizar la efectividad del proceso de auditoría para el sistema electrónico de información documentada. Este documento utiliza la guía proporcionada en la norma ISO 19011 y sugiere enfoques que pueden ser utilizados por los auditores de la norma ISO 9001 y otras normas del sistema de gestión, para verificar la conformidad con la norma mencionada. Los auditores y las organizaciones de auditoría deben realizar los ajustes necesarios para garantizar un enfoque adecuado a medida que realizan los pasos del proceso de auditoría indicados en ISO 19011.

Cabe señalar que la competencia en la auditoría de información electrónica documentada no debe considerarse como una excusa para reducir la duración de la auditoría, sino como un medio para optimizar la eficacia y la eficiencia de la auditoría.

No es la intención de este documento proporcionar pautas para los controles de auditoría asociados con la seguridad de la información. Los interesados ​​en controles adicionales asociados con la seguridad de la información están dirigidos a ISO / IEC 27001, que es un estándar integral para estos asuntos.

2. Iniciación y planificación de la auditoría.

Durante la fase de inicio de la auditoría (es decir, la auditoría de la primera etapa; consulte el documento del Grupo de Prácticas de Auditoría ISO 9001 sobre “La necesidad de un enfoque de auditoría de dos etapas”). La organización de auditoría debe determinar la estructura de la organización que se auditará y el grado. Para lo cual su sistema de gestión utiliza información electrónica documentada. Una organización de sitios múltiples con un proceso centralizado para controlar su información electrónica documentada, o una organización "virtual", requerirá diferentes planes y métodos de auditoría.

La organización de auditoría y el auditado deben acordar cómo los auditores accederán y utilizarán el sistema electrónico de información documentada. Esto puede implicar la consideración de:

- Permitir a los miembros del equipo de auditoría la oportunidad de familiarizarse

con el sistema electrónico de información documentada del auditado (incluida

la programación de tiempo suficiente dentro del plan de auditoría para dicha

orientación).

- Las políticas del auditado para el uso de su infraestructura de tecnología de la

información.

- Instrucciones para acceder y los permisos de seguridad necesarios para acceder

a documentos y registros.

- Salvaguardas y procesos para garantizar que los auditores protegen la

confidencialidad de la información documentada durante y después de la

auditoría.

La organización de auditoría debe asegurarse de que haya suficiente competencia dentro de su equipo de auditoría seleccionado para llevar a cabo una evaluación efectiva del sistema electrónico de información documentada.

3. Revisión de la información documentada,

Dependiendo de si el auditado tiene o no la capacidad de hacer que su información esté disponible a través de una aplicación basada en la web o mediante la transmisión por correo electrónico, la organización de auditoría puede llevar a cabo parte o toda la revisión de la información documentada fuera del sitio; ya sea en línea o mediante la descarga de información electrónica enviada por correo electrónico.

Dependiendo de los factores técnicos y de seguridad, puede que no sea factible realizar una revisión completa del sistema electrónico de información documentada de una organización en línea o mediante la transmisión por correo electrónico de información relevante, antes de llegar al sitio. En tales casos, las actividades de preparación de la auditoría que requieren una revisión de la información electrónica tendrían que ocurrir en las instalaciones del auditado durante la auditoría de la etapa 1.

4. Actividades de operación en el sitio

El enfoque de auditoría para los sistemas de información documentados electrónicos dependerá en gran medida de la cantidad de evidencia requerida para determinar la conformidad en forma de información electrónica.

Durante las actividades en el lugar, el rastro del auditor generalmente debe incluir la ubicación física del proceso que se audita. Sin embargo, con un sistema electrónico de información documentada, el tiempo necesario para confirmar la evidencia para determinar si se cumplen o no los requisitos, puede dedicarse a una estación de trabajo informática, que puede no estar ubicada cerca del proceso real.

Cuando las estaciones de trabajo de la computadora están en áreas remotas que no son accesibles en la ubicación del proceso físico, el tiempo de auditoría real en la ubicación física del proceso puede reducirse. Sin embargo, es posible que no sea necesario reducir el tiempo total de la evaluación, dado que se puede realizar una revisión electrónica de la evidencia antes y / o después de confirmar la existencia del proceso físico.

En el caso de que la estación de trabajo informática asociada se coloque de forma remota, se debe prestar especial atención al tiempo requerido para viajar hacia y desde la ubicación física del proceso.

Cuando el proceso depende de la intervención humana, el auditor debe evaluar los métodos empleados para la interacción entre el proceso físico y los medios electrónicos para garantizar la exactitud de la información asociada.

5. Auditoría del control de información electrónica documentada.

La información electrónica que establece el control operacional del sistema de administración puede estar en una variedad de formatos de archivo, dependiendo de las aplicaciones de software que la organización utiliza para generar la información. Los formatos de archivo electrónico incluyen texto, HTML, PDF, etc.

Los formatos de hojas de cálculo y bases de datos también se consideran información documentada electrónica sujeta a los elementos de control del sistema de gestión a ser auditados.

Dada la relativa facilidad con que los usuarios ahora pueden crear hojas de cálculo electrónicas y otra información electrónica, los auditores deben asegurarse de que los procesos que rigen los controles que se aplican a la información impresa en general del sistema de gestión también se emplean para la información electrónica.

Las organizaciones deben emplear métodos adecuados y efectivos dentro del entorno electrónico para garantizar la revisión, aprobación, publicación y distribución adecuadas de la documentación de su sistema de gestión. Estos deben ser consistentes con los métodos para el desarrollo y modificación de la información electrónica.

En muchos casos, las medidas de control también pueden ser características estándar de las aplicaciones de software utilizadas para su creación. Por lo tanto, los auditores deben comprender estos controles específicos de la aplicación en la medida en que se utilicen como base para el cumplimiento del estándar de sistema de gestión aplicable.

Dada la mayor capacidad para modificar, actualizar, reformatear y mejorar la información documentada dentro de un sistema electrónico de información documentada, los auditores deben prestar especial atención a los elementos de control, como la identificación y el nivel de revisión.

Como los medios electrónicos facilitan una mayor tasa de modificaciones, los auditores deben verificar que los controles que se emplean para la gestión de la información obsoleta se consideran dentro de los procesos de control de las organizaciones.

Los auditores deben verificar que existe información para proporcionar orientación a los usuarios con respecto a los aspectos funcionales y de control asociados con la información electrónica. Además, los requisitos de "punto de uso" asociados con los estándares del sistema de gestión aplicables generalmente serán abordados en parte por las políticas de acceso de la organización. Los auditores deben entender los procesos de la organización con respecto a los privilegios de los usuarios, ya que estos se convierten en factores importantes para implementar adecuadamente los procesos de la organización.

La comunicación electrónica externa con proveedores externos, clientes y otras partes interesadas puede implicar el intercambio de información documentada. Dado que la información documentada puede contener parámetros clave que especifican el funcionamiento de los procesos de la organización, los auditores deben verificar el grado en que estos se introducen y controlan formalmente dentro del sistema electrónico de información documentada.

Los auditores deben revisar los métodos empleados por la organización para capturar los resultados, a fin de garantizar que las actividades proporcionen suficiente confianza en la exactitud de la información.

Al evaluar los controles de la organización con respecto a la retención y el almacenamiento de información documentada, los auditores deben verificar si las organizaciones comprenden su capacidad de almacenamiento en comparación con:

- La tasa de generación de información,

- Los plazos de retención,

- La tasa de eliminación de registros, ya que estos factores pueden afectar el

correcto funcionamiento del sistema electrónico de información documentado.

Dado que la base de conocimientos y el desempeño de la organización pueden estar casi en su totalidad en registros electrónicos, los auditores deben revisar los enfoques de las organizaciones para asegurar la información contenida en medios electrónicos. Para obtener más información sobre la seguridad de la información, consulte ISO / IEC 27001.

6. Recursos

A medida que las organizaciones migran a usar un sistema electrónico de información documentada, el I.T. el papel de la función se vuelve vital. Los auditores deben verificar si la organización ha dedicado la adecuada I.T. recursos (incluida la infraestructura) para garantizar que el sistema funcione de manera continua y eficaz.

Los auditores también deben verificar si la organización ha definido adecuadamente el nivel de interacción, apoyo y participación de I.T. Personal en asuntos relacionados con el establecimiento, implementación y mantenimiento del sistema electrónico de información documentada.

Como parte de la verificación de la asignación de recursos apropiados, los auditores deben evaluar cómo la organización aborda la competencia requerida de las personas para operar hardware y software para ejecutar el sistema electrónico de información documentada.

Durante el establecimiento de un sistema electrónico de información documentada, es habitual que existan sistemas paralelos (en papel y electrónicos) durante un período de tiempo para permitir que los usuarios se adapten. En estos casos, el auditor debe verificar los enfoques de la organización para garantizar que el sistema se esté asimilando y utilizando realmente.

La complejidad de las infraestructuras de TI de una organización variará, dependiendo de la naturaleza y complejidad de su negocio. Los auditores deben verificar los procesos de mantenimiento del sistema de una organización para su plataforma de TI.

Además, los auditores deben verificar cómo la organización aborda los incidentes de inactividad del sistema, ya que esto afectará el funcionamiento normal del sistema electrónico de información documentada. Los auditores deben evaluar si la organización tiene o no sistemas formales de respaldo, y si estos son revisados ​​y probados periódicamente para verificar su idoneidad.

En relación con el software, los auditores deben verificar los controles establecidos para el software interno, el software externo, las licencias de software y las actualizaciones de software. Dado que el software puede considerarse dinámico, las pautas provistas anteriormente para la auditoría de información electrónica también serían aplicables a este.

En la medida en que las organizaciones utilicen software para su sistema electrónico de información documentada, los auditores deben revisar la funcionalidad de las aplicaciones y su relación con los elementos del sistema de gestión definidos en los criterios aplicables.

Como los factores ambientales pueden afectar el funcionamiento de una plataforma de TI, las organizaciones deben tomar medidas para protegerlos contra tales factores. Esto puede ir desde la necesidad de instalaciones o carcasas adecuadas hasta la necesidad de fuentes de alimentación ininterrumpidas (UPS). Los auditores deben evaluar si los controles de la organización tienen en cuenta aspectos como el mantenimiento de las instalaciones, la temperatura, la humedad, etc., en la medida en que estos se relacionen con el funcionamiento del sistema electrónico de información documentada.

7. Comunicación electrónica interna y externa.

A medida que aumentan las opciones disponibles y la facilidad de uso de la comunicación electrónica, las organizaciones deben implementar los controles necesarios para garantizar la coherencia en su uso y para satisfacer los requisitos de su sistema electrónico de información documentada y el estándar de sistema de gestión aplicable.

Cuando se utilizan las intranets, el correo electrónico y la mensajería instantánea para satisfacer los requisitos del sistema electrónico de información documentada, los auditores deben verificar que los procesos abordan las circunstancias en las que se emplearían estos medios. Además, si los resultados de la comunicación electrónica interna se utilizan para satisfacer los criterios de auditoría, los auditores deben verificar que se estén aplicando procesos para el control de la información electrónica.

Cuando la organización se apoya en su I.T. La infraestructura para las comunicaciones electrónicas con sus clientes (por ejemplo, para el comercio electrónico), los proveedores externos (compras electrónicas), los sitios externos y otras partes interesadas, el auditor debe verificar que la metodología y los procesos para estas comunicaciones y las transacciones asociadas se aborden formalmente.

8. Sistemas de gestión de sitios múltiples

Las organizaciones que operan a través de múltiples sitios (o desde una ubicación central a sitios satelitales) generalmente mantienen las comunicaciones y comparten el proceso y procesan los resultados con sus diversas ubicaciones a través de medios electrónicos, como Internet, intranet, correo electrónico y mensajería instantánea.

Cuando el I.T. La plataforma y sus aplicaciones de software asociadas se utilizan para compartir información pertinente a los criterios de auditoría. Los auditores deben comprender los diferentes medios de red empleados por la organización en la medida en que sea necesario para determinar si el sistema electrónico de información documentada cumple con los criterios de auditoría.

Los auditores deben verificar si los controles sobre un sistema de administración de sitios múltiples se abordan y establecen adecuadamente dentro de los procesos de la organización.

9. Competencia del auditor

La confiabilidad del proceso de auditoría para la información documentada electrónica dependerá de la capacidad de los auditores para comprender las tendencias en I.T. a medida que las organizaciones confían cada vez más en software para monitorear y controlar sus operaciones.

Las organizaciones auditoras deben tomar las medidas necesarias, incluida la provisión de capacitación, para abordar las necesidades generales e individuales de su base de auditores con respecto a:

- Tendencias generales en I.T. Eso puede impactar la operación de los sistemas

de gestión.

- Consideraciones específicas de auditoría para cada una de las audiencias

A medida que las innovaciones en el I.T. Los sectores son relativamente

rápidos en comparación con los cambios en los criterios de auditoría, los

auditores y las organizaciones de auditoría tienen el reto de tener una

comprensión práctica de las tendencias asociadas y cómo pueden ser

aplicables y utilizadas dentro de un sistema electrónico de información

documentada.

A la luz de las innovaciones que influyen en el funcionamiento de un sistema electrónico de información documentado, las organizaciones de auditoría deben determinar si el equipo de auditoría posee la experiencia necesaria para ser eficaz en una auditoría determinada o si se requiere la asistencia de un experto técnico.

Para obtener más información sobre el Grupo de prácticas de auditoría ISO 9001, consulte el documento: Introducción al Grupo de prácticas de auditoría ISO 9001.

La retroalimentación de los usuarios será utilizada por el Grupo de Prácticas de Auditoría ISO 9001 para determinar si se deben desarrollar documentos de orientación adicionales, o si se deben revisar estos actuales.

Los comentarios sobre los trabajos o presentaciones se pueden enviar a la siguiente dirección de correo electrónico: [charles.corrie@bsigroup.com](mailto:charles.corrie@bsigroup.com).

Los otros documentos y presentaciones del Grupo de Prácticas de Auditoría ISO 9001 se pueden descargar de los sitios web:

www.iaf.nu [www.iso.org/tc176/ISO9001AuditingPracticesGroup](http://www.iso.org/tc176/ISO9001AuditingPracticesGroup)

Renuncia

Este documento no ha sido sujeto a un proceso de aprobación por parte de la Organización Internacional de Normalización (ISO), el Comité Técnico 176 de la ISO o el Foro Internacional de Acreditación (IAF).

La información contenida en ella está disponible para fines educativos y de comunicación. El Grupo de Prácticas de Auditoría ISO 9001 no se responsabiliza de los errores, omisiones u otras responsabilidades que puedan surgir de la provisión o el uso posterior de dicha información.

© ISO & IAF 2016 - Todos los derechos reservados.

www.iaf.nu; [www.iso.org/tc176/ISO9001AuditingPracticesGroup](http://www.iso.org/tc176/ISO9001AuditingPracticesGroup)

.