



CERTIFICACIÓN DE SISTEMAS DE INOCUIDAD DE LOS ALIMENTOS

**ANEXO 5: REQUISITOS DEL OC PARA EL USO DE
TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
(TIC)**

ÍNDICE

1. Proposito.....	1
2. Alcance.....	2
3. Realización de auditorías mediante la utilización de las TIC	2
4. Principios generales	3
5. Equipo de auditoría	8

1. PROPOSITO

En el presente anexo se describen los requisitos para la utilización de tecnologías de la información y la comunicación (TIC) por los organismos de certificación vinculados a las actividades de auditoría de la FSSC 22000.

2. ALCANCE

El alcance de este documento abarca lo siguiente:

- La realización de auditorías de la FSSC 22000 utilizando las tecnologías de la información y la comunicación (TIC)
- Requisitos y actividades del auditor del OC

El uso de las TIC supone el uso de la tecnología para reunir, almacenar, recuperar, procesar, analizar y transmitir información. Abarca software y hardware, como teléfonos inteligentes, tabletas, computadoras portátiles, computadoras de escritorio, drones, cámaras de video, tecnología vestible, inteligencia artificial y otros. El uso de las TIC puede ser apropiado para la auditoría/evaluación tanto a nivel local como remotamente.

A medida que evoluciona la tecnología y aumentan las limitaciones de tiempo de las empresas, es necesario considerar métodos alternativos para llevar a cabo las actividades de auditoría sin dejar de alcanzar los objetivos de la auditoría y garantizando un proceso de auditoría robusto.

El Documento Obligatorio (MD) 4 del IAF para la *Utilización de las tecnologías de la información y la comunicación (TIC) con fines de auditoría/evaluación* (última versión) debe utilizarse por los OC como documento normativo junto con los requisitos establecidos en el presente anexo.

3. REALIZACIÓN DE AUDITORÍAS MEDIANTE LA UTILIZACIÓN DE LAS TIC

El método estándar para llevar a cabo las auditorías de la FSSC 22000 es a través de auditorías completas in situ como se describe en la Parte 3 del Esquema. Una opción alternativa y voluntaria puede aplicarse ahora cuando se cumplen los criterios, realizando la auditoría FSSC 22000 en un proceso dividido utilizando la TIC. Esto se conoce como el planteamiento de auditoría mediante TIC, que es voluntario y se debe acordar mutuamente entre el OC y la organización certificada antes de la auditoría.

El planteamiento de auditoría mediante TIC consta de dos (2) componentes, que deberían ejecutarse en el siguiente orden:

Paso 1: componente de auditoría remota, que consiste en una revisión de documentos y entrevistas con el personal clave mediante el uso de las TIC.

Paso 2: componente de auditoría in situ centrada en la aplicación y verificación del SGIA (incluido el HACCP), los PPR, la inspección física del proceso de producción y cualquier otro requisito que no se haya cubierto durante la auditoría remota.

Aunque es preferible realizar primero el componente de auditoría remota, es posible invertir la secuencia y comenzar con el componente de auditoría in situ. Si se invierte la secuencia, se puede requerir al auditor que (re)verifique una actividad de producto/proceso in situ, basándose en el resultado del componente de auditoría remota, lo que podría dar lugar a que el auditor tuviera que regresar al sitio para verificar esta actividad. En este caso, el OC y la organización deben aceptar este riesgo por escrito antes de la ejecución de la Auditoría mediante uso de TIC en este orden. Si el auditor tuviera que regresar al sitio para la actividad de verificación, esta se debe seguir considerando parte de la auditoría regular y completará dentro de un marco total de 30 días. La auditoría no se considerará completa hasta que se hayan ejecutado todos los componentes.

Los componentes de la auditoría (remota + in situ) también pueden ejecutarse al mismo tiempo si se recurre a un equipo de auditoría.

Durante la **auditoría remota**, las actividades de evaluación se realizan desde un lugar distinto de la ubicación física de la organización auditada, mientras que durante la **auditoría in situ**, las actividades de evaluación se realizan en la ubicación física de la organización auditada.

El OC debe realizar una evaluación de viabilidad para determinar, junto con la organización certificada, si el planteamiento de auditoría mediante TIC es una opción viable. El OC debe tener de procedimientos documentados que incluyan criterios para evaluar y aprobar el planteamiento de auditoría mediante TIC. Esta evaluación de viabilidad debe llevarse a cabo y documentarse antes de la auditoría, teniendo en cuenta a los miembros del equipo de auditoría y a la organización auditada.

Al realizar la evaluación de viabilidad se debe tener en cuenta lo siguiente:

- a) La madurez del SGIA de la organización certificada y su historial de desempeño;
- b) Si la organización certificada permite y da cabida a la actividad de auditoría remota (es decir, disponibilidad de registros en formato electrónico o lector de documentos), incluidas la protección de datos y las medidas de seguridad;
- c) Las herramientas TIC que se utilizarán;
- d) Si la organización certificada y/o el OC tienen representantes capaces de comunicarse en la misma lengua;
- e) Si el OC y la organización certificada tienen la capacidad y la posibilidad de realizar la auditoría remota en el medio/foro elegido para la auditoría remota; y
- f) Impacto en la duración y la planificación de la auditoría, por ejemplo, en los casos en que se requiera más tiempo debido a la utilización de TIC.

4. PRINCIPIOS GENERALES

- a) Si se considera que el planteamiento de auditoría mediante TIC es una opción viable, los medios de TIC que se utilicen deben ser probados con la organización certificada antes de la auditoría remota planificada para confirmar que la TIC es apropiada, adecuada y eficaz. La viabilidad también depende de la calidad de la conexión en línea. Un ancho de banda débil o una capacidad de hardware limitada pueden retardar el proceso hasta el punto de la ineficiencia.

- b) Antes de la auditoría remota, se debe proporcionar al auditor y a cualquier otro miembro del equipo de auditoría el apoyo y la capacitación adecuados sobre el uso de las TIC. Los registros de estas capacitaciones deben ser conservados por el OC y cargados en el registro del auditor en Assurance Platform.
- c) Se deben acatar los requisitos del IAF MD 4. Este documento obligatorio define las reglas que los Organismos de Certificación y sus auditores deben seguir para garantizar que las TIC se utilizan para optimizar la eficiencia y eficacia de la auditoría/evaluación, al mismo tiempo que se apoya y mantiene la integridad del proceso de auditoría.
- d) El OC debe incluir los requisitos del MD 4 del IAF en sus procedimientos para el uso de las TIC y la competencia del personal.
- e) Seguridad y confidencialidad de los datos: para prepararse para el uso de las TIC, se deben identificar todos los requisitos legales de certificación y de los clientes relacionados con la confidencialidad, la seguridad y la protección de los datos, y se deberían tomar medidas para garantizar su aplicación efectiva. Esto implica que tanto el auditor como el auditado estén de acuerdo con el uso de las TIC y con las medidas adoptadas para cumplir estos requisitos.
- f) Tanto la auditoría remota como la auditoría in situ deben ser realizadas por un auditor o auditores calificados en FSSC 22000. El equipo de auditoría debe poseer la competencia combinada para las subcategorías de la cadena alimentaria que respaldan el alcance de la auditoría. Los auditores que realicen el componente in situ de la auditoría, así como cualquier actividad relacionada con el producto/proceso (evaluación de las actividades del producto/proceso, estudios de HACCP, etc.) deben poseer competencias para las subcategorías de la cadena alimentaria, o para la categoría si no existe ninguna subcategoría, vinculadas al alcance de la auditoría.
- g) El componente remoto de la auditoría durará típicamente de 0.5-1 día, y la auditoría de verificación in situ tomará el resto de la duración total de la auditoría anual ordinaria. El componente in situ de la auditoría no puede ser inferior a 1 día y debe ser al menos el 50 % de la duración total de la auditoría. Al determinar la cantidad de tiempo que se dedica in situ y remotamente, se debe tomar en cuenta los resultados de la evaluación de viabilidad y el historial de desempeño de la organización (incluidas las quejas y la recuperación de producto del mercado). Por ejemplo, si la evaluación de viabilidad demostró que es posible realizar una auditoría remota, pero el desempeño histórico de la organización ha sido motivo de preocupación, entonces se espera que aumente la proporción de tiempo que se dedica in situ.
- h) La duración total de la auditoría se basa en el cálculo de la Parte 3 de las normas del Esquema se debe cumplir entre el componente de auditoría remota y el componente de auditoría in situ. Cuando se aplique el redondeo, las duraciones deben redondearse hacia arriba al medio día más cercano, teniendo en cuenta que podría requerirse tiempo adicional para realizar el componente de auditoría remota. La duración total de la auditoría no incluye las actividades de preparación o de preparación de informes y se requiere tiempo adicional para estas actividades, tal como se define en la Parte 3 del Esquema.
- i) Al preparar el plan de auditoría para el componente de auditoría remota, se deberían tomar en cuenta las duraciones apropiadas y permitir pausas más frecuentes para mejorar la atención y reducir la tensión ocular. Estos descansos no pueden contarse en la duración de la auditoría.
- j) Si se consume tiempo en cuestiones como la inactividad de la red, interrupciones o retrasos inesperados, problemas de accesibilidad u otros desafíos de TIC, este tiempo no

debe contarse como duración de la auditoría. Se establecerán disposiciones para garantizar la duración de la auditoría.

- k) Se recomienda que los componentes de la auditoría remota y la auditoría in situ tengan lugar lo más cerca posible, pero el plazo máximo para la realización de la auditoría (remota + in situ) no debe exceder en ningún caso los 30 días naturales.
- l) Como excepción, y solo en caso de los acontecimientos graves definidos por el Esquema, el plazo para la finalización de la auditoría podrá ampliarse hasta un máximo de 90 días naturales, sobre la base de un proceso de concesión claro y documentado y de una evaluación de los riesgos por parte del OC. La evaluación de riesgos debe considerar como mínimo los elementos de la sección 3 del Documento de Información (ID) 3 del IAF *Gestión de eventos o circunstancias extraordinarias que afectan los OA, OEC y organizaciones certificadas*. La extensión solo se permite siempre y cuando la eficiencia e integridad de la auditoría no se vean comprometidas. Si el OC hace concesiones y se aplica el plazo de 90 días, la evaluación de riesgos se debe cargar en Assurance Platform como parte de la documentación de la auditoría.
- m) En todos los casos en que las TIC utilizadas no funcionen correctamente, impidan o dificulten una auditoría robusta, se debe abortar la auditoría y se determinarán las acciones de seguimiento adecuadas.
- n) Si se produjera un acontecimiento grave después de que haya comenzado un planteamiento de auditoría mediante TIC y sea necesario convertir la auditoría en una auditoría totalmente remota, el OC debe solicitar una excepción a la Fundación. En el supuesto de que se concediera una excepción, el OC debe seguir los requisitos de la agenda para auditorías totalmente remotas, incluida la realización de una evaluación de riesgos (consulte la Parte 3, sección 5.10, del Esquema) y es necesario llevar a cabo una evaluación de viabilidad adicional para garantizar que las TIC sean adecuadas para realizar la auditoría totalmente remota, incluida la auditoría de los procesos de producción.

4.1 APLICABILIDAD

Las auditorías mediante TIC pueden aplicarse en el caso de las auditorías anuales regulares de la FSSC 22000 (auditorías de vigilancia y recertificación) como parte del proceso de certificación rutinario y es adicional a la Parte 3 del Esquema.

El uso de las TIC puede aplicarse a las auditorías de la Etapa 1 en circunstancias o acontecimientos excepcionales, como se describe a continuación, y para las auditorías de la oficina central/corporativo en las que las funciones corporativas se controlan por separado.

En el año en que se requiera realizar una auditoría no anunciada, se podrá utilizar la auditoría mediante TIC descrito en este Anexo, aplicando al mismo tiempo los requisitos de la Parte 3, sección 5.4 de del Esquema. El prerequisite establece que auditoría componente de la auditoría in situ se debe realizara primero, seguida directamente por el componente de auditoría remota con un período máximo de 48 horas entre los dos componentes de la auditoría.

4.1.1 AUDITORÍAS INICIALES

En circunstancias o acontecimientos excepcionales, la totalidad o parte de la Etapa 1 puede realizarse fuera de sitio o a distancia mediante el uso de las TIC y debe ser totalmente justificable (ISO 22003-1:2022, cláusula 9.3.5). Se deben cumplir los objetivos de la auditoría de la Etapa 1 según la norma ISO17021-1 (9.3.1.2.2) y para ello se debe incluir las TIC (por ejemplo, video en directo) para observar también los procesos de producción, el ambiente de trabajo y las instalaciones. En el informe de auditoría de la Etapa 1 se debe hacer referencia a que la auditoría

fue realizada de manera completamente remota, así como las herramientas de TIC utilizadas y se incluirá una confirmación de que los objetivos se han alcanzado.

La auditoría de la Etapa 2 se debe llevar a cabo como una auditoría completa in situ dentro de los 6 meses siguientes a la Etapa 1, o si no, se debe repetir la Etapa 1. No está permitido el planteamiento de auditoría mediante TIC para la auditoría de la Etapa 2.

4.1.2 AUDITORÍAS DE VIGILANCIA

Podrán realizarse auditorías de vigilancia anuales utilizando el planteamiento de auditoría mediante TIC. La auditoría completa (remota + in situ) se debe completar dentro del año natural.

Si se aplica el planteamiento de auditoría mediante TIC a la primera auditoría de vigilancia tras una certificación inicial, el proceso debe planificarse para garantizar que la auditoría completa (remota + in situ) se realice antes o en un plazo máximo 12 meses a partir de la fecha de la decisión de certificación de la auditoría inicial. En el supuesto de que no se haya ejecutado la auditoría completa en el plazo de 12 meses, se debe suspender el certificado.

4.1.3 AUDITORÍAS DE RECERTIFICACIÓN

Las auditorías de recertificación anuales pueden realizarse utilizando el planteamiento de auditoría mediante TIC. El componente de auditoría remota combinado con el componente de auditoría in situ constituyen una auditoría de recertificación completa y ambos componentes deben completarse antes de la expiración del certificado existente. Se aplican los requisitos de la norma ISO/IEC 17021-1:2015, cláusula 9.6.3.2.

4.2 PROCESO DE AUDITORÍA

La auditoría (remota + in situ) debe realizarse por auditores calificados en la FSSC 22000 que cumplan los requisitos de competencia relacionados con el alcance de la certificación. En todos los casos, la auditoría in situ debe ser llevada a cabo por un auditor líder calificado para FSSC 22000 con la subcategoría. Si los componentes a distancia e in situ se ejecutan en momentos diferentes y por auditores distintos, el OC debe contar con un proceso de traspaso/comunicación adecuado.

4.2.1 COMPONENTE DE AUDITORÍA REMOTA

El componente de auditoría remota debe incluir una revisión de documentos y entrevistas con el personal clave.

A continuación, se ofrecen ejemplos de lo que puede incluirse como parte de la revisión de documentos realizada durante el componente de auditoría remota:

- Revisión de documentos/procedimientos;
- Cambios clave desde la última auditoría (cuando corresponda);
- Recuperación de productos y quejas significativas;
- Estado con respecto a los objetivos del SGIA y el desempeño de los procesos clave, la revisión de la dirección y las auditorías internas.

4.2.2 COMPONENTE DE AUDITORÍA IN SITU

El componente de auditoría in situ sirve como auditoría de verificación para la implementación del sistema de gestión de la inocuidad de los alimentos (SGIA), centrándose en los procesos y el ambiente de producción, así como en el resto de las cláusulas no incluidas en el componente de auditoría remota.

El componente de auditoría in situ debe incluir como mínimo la inspección/verificación física de los PPR, la prueba de trazabilidad y la implementación del SGIA. Esta última incluye, pero no se limita, a el sistema del HACCP, por ejemplo, el funcionamiento eficaz de los PPR, la verificación del diagrama de flujo del proceso, la vigilancia y la verificación del PPRO y los PCC. Tal vez sea necesario volver a examinar partes de la auditoría remota para garantizar la aplicación de los requisitos.

Todos los requisitos del Esquema se deben cubrir entre los componentes remoto e in situ de la auditoría y reflejar con claridad en los planes de auditoría, el programa de auditoría y el informe final de auditoría.

4.2.3 GESTIÓN DE NO CONFORMIDADES

Cualquier no conformidad identificada durante la auditoría (remota e in situ) se debe abordar de acuerdo con los requisitos del Esquema, incluidos la clasificación y los plazos, y registrarse en el informe de NC (consulte el Anexo 2).

- i. Cuando la auditoría (remota + in situ) se completa en un plazo de 30 días naturales, se elabora un informe de no conformidad y el plazo para el cierre de la no conformidad comienza al final del último componente de auditoría. Toda no conformidad identificada en el transcurso de la auditoría se debe comunicar a la organización de manera oportuna. El OC podrá optar por proporcionar un informe de NC provisional a la organización al final del primer componente de auditoría ejecutado.
- ii. En caso de un acontecimiento grave y cuando se superen los 30 días naturales para la finalización de la auditoría (consulte la excepción en el apartado 3.1 (I)), toda no conformidad identificada como parte del primer componente de auditoría remota se debe registrar y se dejará una copia del informe de no conformidad a la organización certificada al final del primer componente de auditoría. El plazo para el cierre de las no conformidades comienza al final del primer componente de auditoría. El informe de NC elaborado tras el último componente de auditoría debe contener una descripción general de todas las no conformidades planteadas, incluidas las no conformidades planteadas en el primer componente de auditoría para proporcionar un registro consolidado. El plazo para el cierre de las NC identificadas en el último componente de auditoría comienza al final del último componente de auditoría.
- iii. Cuando se identifique una no conformidad crítica en cualquier momento de la auditoría (remota o in situ), se debe suspender el certificado y se requerirá una nueva auditoría in situ completa para levantar la suspensión dentro de un plazo de 6 meses.

Se pueden utilizar herramientas de TIC para cerrar las no conformidades menores o mayores, dependiendo de la naturaleza de la no conformidad y de la confiabilidad de las TIC. El OC debe ser capaz de demostrar que los métodos utilizados son adecuados para las acciones medida resultantes. Las no conformidades críticas requieren una auditoría de seguimiento in situ en todos los casos.

4.2.4 INFORME DE AUDITORÍA

Se elabora un informe de auditoría que cubre tanto los componentes de la auditoría remota como los de la auditoría in situ. El informe de auditoría debe identificar claramente el grado en que se ha utilizado cualquier TIC para llevar a cabo la auditoría y la eficacia de las TIC para alcanzar los objetivos de la auditoría. El informe de auditoría debe incluir toda la información resumida, las conclusiones y los detalles de no conformidad de los componentes de auditoría tanto remota como in situ, abarcando todos los requisitos normativos del Esquema y cumpliendo los requisitos establecidos en el Anexo 2 del Esquema. El informe también debe hacer referencia a las fechas y la duración de los componentes de auditoría in situ y remota y al auditor o auditores involucrados en ambos componentes.

El paquete de auditoría completo, que consiste en la documentación de la auditoría remota y la auditoría in situ, se debe cargar en Assurance Platform en un plazo no mayor de 2 meses a partir del último día de la auditoría completa. La Fundación dará instrucciones por separado sobre el proceso y los requisitos para cargar la información de la auditoría y las no conformidades en Assurance Platform.

La auditoría de certificación solo concluirá una vez que se hayan completado con éxito los componentes tanto de auditoría remota como de auditoría in situ. Una vez concluida la auditoría completa (componentes remoto e in situ) y tras una decisión de certificación positiva por parte del OC, el proceso de auditoría se completa y, cuando proceda, se puede emitir un nuevo certificado.

5. EQUIPO DE AUDITORÍA

5.1 TESTIFICACIÓN DE AUDITORES

Cuando se disponga de las herramientas de TIC apropiadas, esta tecnología también podrá utilizarse para la testificación a distancia de los auditores FSSC 22000 ya calificados, como parte de los requisitos de mantenimiento de la competencia (auditoría de testificación cada tres años) y el proceso de recalificación.

Lo mismo se aplica a los auditores ya calificados en la FSSC 22000 que se trasladan a otro OC. Cuando el nuevo OC considere que la testificación a distancia es suficientemente robusta, el nuevo OC puede utilizar una auditoría de testificación remota para aprobar al auditor de la FSSC 22000. No se permite la testificación remota para la aprobación inicial del auditor de la FSSC 22000 (auditores nuevos en la FSSC 22000).

En todos los casos en que se utilicen herramientas de TIC, el OC necesita asegurarse de que la tecnología sea apropiada y permita al auditor de testificación observar la auditoría de certificación completa de la FSSC 22000, incluida la reunión de apertura, la revisión de documentos, la auditoría de las instalaciones in situ y la reunión de cierre. Es necesario que en el informe de auditoría de testificación quede claramente reflejado que esta se realizó de manera remota y qué tecnología remota se utilizó. Se requerirá autorización de la organización certificada para realizar la auditoría de testificación de esta manera y se aplicarán los requisitos normales de confidencialidad. La tecnología debe probarse de antemano y el auditor de testificación y el auditor recibirán capacitación en la utilización de la tecnología, como se exige en la norma MD 4 del IAF. En todos los casos en que la tecnología utilizada no funcione correctamente o impida o dificulte una auditoría robusta, se debe abortar la auditoría de testificación y el OC determinará las acciones de seguimiento adecuadas.

5.2 USO DE EXPERTOS TÉCNICOS

Se permite la incorporación de expertos técnicos a la auditoría remota utilizando herramientas de TIC, siempre y cuando el OC haya determinado que las herramientas de TIC son apropiadas y suficientes para cumplir los objetivos de la auditoría y la organización certificada está de acuerdo con la actividad de auditoría remota. La tecnología necesita probarse de antemano y tanto el experto técnico como el auditor deben recibir capacitación en la utilización de la tecnología, tal como se exige en el MD 4 del IAF. En todos los casos en que la tecnología utilizada no funcione correctamente o impida o dificulte una auditoría robusta, el OC debe tomar medidas alternativas para garantizar que se pueda concluir el proceso de auditoría completo o se debe abortar la auditoría.