DE:	Dirección Técnica Internacional
PARA:	Organismos de Certificación de Sistemas de Gestión de la Seguridad de la Información - SGSI
ASUNTO:	Plan de Transición versión 2022 de la norma ISO/IEC 27001
DOCUMENTOS RELACIONADOS:	ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección a la privacidad – Sistemas de gestión de la seguridad de la información - Requisitos"

1. PUBLICACIÓN DE LA ACTUALIZACIÓN DE LA NORMA ISO/IEC 27001:2022

El día **25 de octubre de 2022** se realizó la publicación de la norma ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección a la privacidad – Sistemas de gestión de la seguridad de la información - Requisitos" por parte de la Organización Internacional de Normalización – ISO y la Comisión Electrotécnica Internacional - IEC, como resultado de la labor del Comité Técnico ISO/IEC JTC 1/SC 27 *"Information security, cybersecurity and privacy protection"*, teniendo como antecesores los documentos normativos ISO/IEC 27001:2013, ISO/IEC 27001:2013/Cor 1:2014, ISO/IEC 27001:2013/Cor 2:2015 e ISO/IEC 27001:2013/DAmd1 de julio de 2022.

La norma ISO/IEC 27001 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en el contexto de la organización. Este documento también incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información conforme a las necesidades de la organización.

2. CONSIDERACIONES DEL FORO INTERNACIONAL DE ACREDITACIÓN – IAF

Tras su publicación, el Foro Internacional de Acreditación – IAF, del cual ONAC es miembro, estableció mediante el documento mandatorio IAF MD 26:2023 *"Transition Requirements for ISO/IEC 27001:2022"*, aprobado el día 15 de febrero de 2023, un periodo de transición de **36 meses** a la nueva versión de la norma ISO/IEC 27001. De esta manera, la fecha máxima para estar en conformidad con esta nueva versión es el **31 de octubre de 2025**.

Dentro de dicho periodo, este documento indica los siguientes tiempos de transición para los Organismos de Acreditación:

- "Los Organismos de Acreditación deben estar listos para evaluar con base en la ISO/IEC 27001:2022 al finalizar los seis (6) meses después de la publicación del documento, siendo este el **30 de abril de 2023.**
- Las evaluaciones iniciales realizadas por los Organismos de Acreditación se llevarán a cabo haciendo uso únicamente de la norma ISO/IEC 27001:2022 a más tardar seis (6) meses después de la publicación del documento, siendo la fecha límite el **30 de abril de 2023.**
- Para el **31 de octubre de 2023,** se debe haber cumplido la totalidad de la transición de los Organismos Evaluadores de Conformidad – OEC a la nueva versión de la norma ISO/IEC 27001."

De igual forma, se estipulan los siguientes tiempos de transición para los Organismos Evaluadores de Conformidad:

- "Las actividades de certificación inicial y recertificación realizadas por los Organismos de Evaluación de la Conformidad se deberán llevar a cabo únicamente con base en la norma ISO/IEC 27001:2022 a más tardar dieciocho (18) meses posteriores a la publicación del documento, teniendo como fecha límite el **30 de abril de 2024.**
- La transición de los clientes certificados por los Organismos de Evaluación de la Conformidad deberá completarse en el curso de los treinta y seis (36) meses posteriores a la publicación del documento, teniendo como fecha límite el **31 de octubre de 2025.**

Para más información, el documento IAF MD 26:2023 " *Transition Requirements for ISO/IEC 27001:2022*"se encuentra disponible en la página web de IAF en el siguiente link: https://iaf.nu/iaf_system/uploads/documents/IAF_MD26_Issue_2_15012023.pdf. En el MD26 se relaciona información adicional sobre los cambios claves con la actualización de la norma ISO/IEC 27001 y detalle de las actividades que se deben realizar por parte del organismo de acreditación y del organismo evaluador de la conformidad para realizar el proceso de transición exitosamente.

3. CONSIDERACIONES DEL ORGANISMO NACIONAL DE ACREDITACIÓN DE COLOMBIA – ONAC

Considerando lo anterior, para el **31 de octubre de 2023**, 12 meses después de la publicación de la nueva versión de la norma, todos los Organismos de Certificación de Sistemas de Gestión de la Seguridad de la Información deben haber demostrado su competencia frente a la aplicación de los requisitos de la norma ISO/IEC 27001:2022. Para ello, deben contar con la decisión del mantenimiento de su condición de acreditado por parte del Comité de Acreditación y concepto favorable por parte del evaluador líder respecto a la implementación eficaz de la norma ISO/IEC 27001:2022 y demás criterios de acreditación que conforman este sub-alcance:

- ISO/IEC 17021-1 "Evaluación de la Conformidad – Requisitos para organismos que proveen auditoria y certificación de sistemas de gestión – Parte 1: Requisitos".
- ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección a la privacidad – Sistemas de gestión de la seguridad de la información - Requisitos".
- ISO/IEC 27006:2015 AMD 1:2020 "Tecnología de la información. Técnicas de seguridad. Requisitos para organismos que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información".
- Documentos mandatorios IAF aplicables.

Una vez se confirme que se ha implementado eficazmente la nueva versión de la ISO/IEC 27001, los Organismos de Certificación de Sistemas de Gestión de la Seguridad de la Información acreditados, de manera gradual, deberán dejar de realizar auditorías iniciales aplicando la norma ISO/IEC 27001:2013, conforme a los acuerdos que el Organismo de Certificación defina para su proceso de transición, respetando los requisitos establecidos por el IAF MD 26:2023 y los lineamientos contenidos en el presente documento.

De acuerdo con lo anterior, a partir del **30 de abril de 2023** los organismos de certificación de sistemas de gestión de la seguridad de la información acreditados podrán solicitar la actualización de este alcance en el marco de su evaluación regular, ya sea seguimiento o reevaluación, o, por medio de una evaluación extraordinaria, para confirmar que han implementado los cambios requeridos para adelantar auditorías del SGSI acorde con lo establecido en la norma ISO/IEC 27001:2022. La solicitud podrán realizarla mediante correo electrónico a la Coordinación Sectorial de Certificaciones: onac@onac.org.co, olga.puentes@onac.org.co, claudia.vela@onac.org.co.

Todas las testificaciones seleccionadas tras la decisión de transición se basarán en la norma ISO/IEC 27001:2022 y se centrarán en evaluar la competencia del Organismo de Evaluación de la Conformidad para llevar a cabo una auditoría basada en ISO/IEC 27001:2022.

Si para el **31 de octubre de 2023** el Comité de Acreditación no ha decidido respecto a la competencia del organismo de certificación de acuerdo con la norma ISO/IEC 27001:2022, se pondrá en consideración del Comité de Acreditación la suspensión de la acreditación para este alcance, siguiendo lo descrito en las Reglas del Servicio de Acreditación RAC-3.0-01 para procedimientos y plazos.

Para este plan de transición, ONAC mantendrá en el Directorio Oficial de Acreditados, la acreditación con las dos versiones de la norma, hasta la culminación del plazo de transición definido por el Foro Internacional de Acreditación – IAF: **31 de octubre de 2025**, fecha a partir de la cual solo estarán publicados aquellos Organismos de Certificación cuyo alcance sea expresado respecto a la conformidad con la norma ISO/IEC 27001:2022.

Por otro lado, los organismos de certificación de sistemas de gestión interesados en acreditarse bajo la norma ISO/IEC 27001 en su más reciente versión, podrán realizar su solicitud a partir del **30 de abril de 2023** por medio del aplicativo SIPSO.

A partir del **30 de abril de 2023** las evaluaciones iniciales realizadas por ONAC en este sub-alcance se llevarán a cabo haciendo uso únicamente de la norma ISO/IEC 27001:2022.

Desde el **30 de abril de 2024** los Organismos de Certificación de SGSI acreditados deberán realizar todas las certificaciones y recertificaciones a sus clientes haciendo uso únicamente de la nueva versión de la norma en mención. En línea con lo anterior, la transición de los clientes certificados por los Organismos de Evaluación de la Conformidad deberá completarse a más tardar el **31 de octubre de 2025.** La actualización del documento de certificación, tras completar de manera exitosa la auditoría de transición, no implica cambios en su ciclo de certificación vigente**.** Todas las certificaciones basadas en la norma ISO/IEC 27001:2013 expirarán o se retirarán al final del período de transición. ONAC verificará el cumplimiento de estas condiciones mediante las evaluaciones regulares del ciclo normal de acreditación.

A continuación, se presenta un gráfico que ilustra las fechas y actividades clave para el proceso de transición a la norma ISO/IEC 27001:2022:

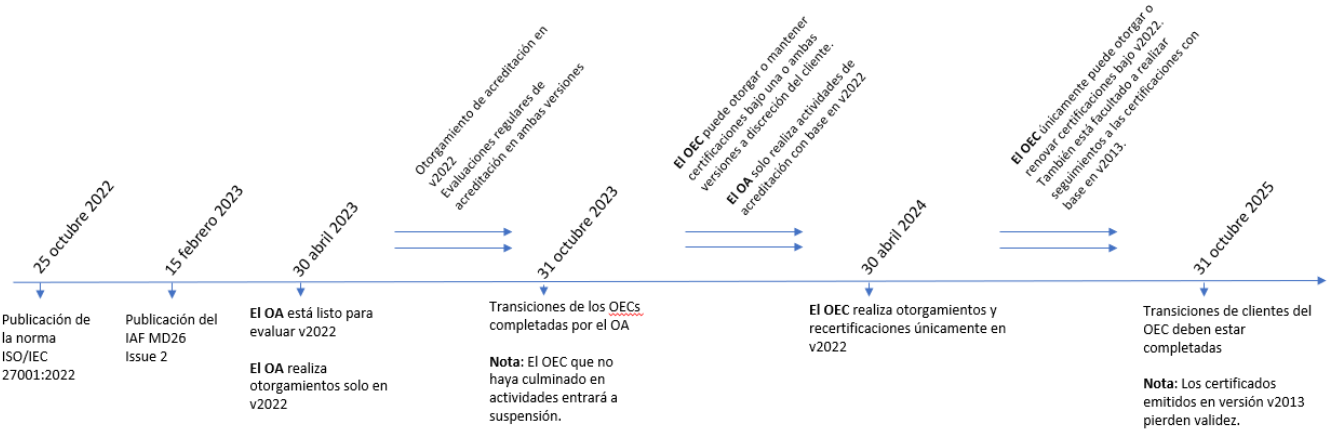

Imagen 1. Línea de tiempo para la transición a la norma ISO/IEC 27001:2022

Los tiempos de esta transición se han planeado considerando los tiempos necesarios para la gestión de contingencias que puedan presentarse durante el proceso de acreditación, sin poner en riesgo su continuidad, y de conformidad a las disposiciones del Foro Internacional de Acreditación – IAF.

CONTROL DE CAMBIOS		
Versión	**Fecha de Aprobación**	**Resumen de Cambios**
1	2023-04-28	Emisión original del documento.
2	2023-06-01	Se incluye texto aclaratorio para la correcta aplicación del lineamiento relacionado con la implementación de la nueva versión de la ISO/IEC 27001 en auditorías iniciales por parte del Organismo de Certificación, una vez se realiza la confirmación de su competencia para certificar con base en la nueva versión de la norma.
3	2023-09-25	Se realiza corrección de la fecha límite de transición de la acreditación de los OEC indicada en el párrafo 5 del numeral *3. CONSIDERACIONES DEL ORGANISMO NACIONAL DE ACREDITACIÓN DE COLOMBIA – ONAC*, acorde a la información registrada en el párrafo 1 del mismo apartado y los lineamientos establecidos por el IAF MD 26. Para asegurar la adecuada interpretación de la información contenida en el *Capítulo 3 Calendario clave* del IAF MD 26, se incluye un gráfico con la línea de tiempo y actividades relevantes en torno al proceso de transición.

ELABORÓ:	REVISÓ:	APROBÓ:
Fecha: 2023-09-22 Profesional Experto Investigación y Desarrollo	Fecha: 2023-09-22 Coordinadora Sectorial Certificación	Fecha: 2023-09-25 Director Técnico Internacional