PLAN DE TRANSICIÓN DE LOS CRITERIOS DE ACREDITACIÓN PARA LAS ENTIDADES DE CERTIFICACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN A LA NUEVA NORMA ISO/IEC 27006-1:2024.

En marzo de 2024 se aprobó la nueva norma ISO/IEC 27006-1:2024 "*Information security, cybersecurity and privacy protection - Requirements for bodies providing audit and certification of information security management systems - Part 1: General*".

IAF ha establecido un calendario para la transición (documento "IAF MD 29:2024"), acordándose un periodo de implantación de la nueva norma **ISO/IEC 27006-1:2024** de 24 meses desde su fecha de publicación. Esto, en términos prácticos, implica que antes del **31 de marzo de 2026** las entidades acreditadas en el esquema deben haber demostrado el cumplimiento con los requisitos de la nueva norma.

Por todo ello y para permitir una transición ordenada de una norma a otra, ENAC ha establecido el siguiente plan de transición:

1. Desde el **1 de diciembre del 2024** todas las auditorías se realizarán de acuerdo a los requisitos de la norma **ISO/IEC 27006-1:2024**.

ENTIDADES NO ACREDITADAS

2. A partir del **1 de septiembre de 2024** todas las solicitudes serán con respecto a **ISO/IEC 27006-1:2024.** Los solicitantes anteriores deberán tener en cuenta además lo contemplado en el punto 1.

ENTIDADES ACREDITADAS

3. Hasta el **31 de marzo de 2026**, las EC podrán seguir desempeñando sus actividades, aunque el anexo técnico de su certificado de acreditación no haga aún referencia a la **ISO/IEC 27006-1:2024**. A partir de esa fecha no podrán mantenerse acreditaciones sin referencia a la nueva norma.

4. Durante dicho periodo, las EC deberán identificar los cambios y recoger en sus procesos los requisitos de la nueva norma (ver Anexo I), elaborando un plan de transición al respecto y comunicando a sus clientes tanto los aspectos necesarios como sus plazos.

5. La actualización de la acreditación se producirá a solicitud de la entidad, presentando a ENAC evidencias de la implantación efectiva de los nuevos requisitos, identificados en su correspondiente análisis de las diferencias respecto de la anterior versión de la norma. ENAC ofrece dos alternativas para evaluar el cumplimiento de los requisitos de la nueva versión de la norma:

    i. durante la siguiente visita planificada de seguimiento o reevaluación de la acreditación, tras la publicación de este plan, o

    ii. mediante una evaluación específica, cuando la entidad así lo solicite enviando un correo electrónico a secent@enac.es con al menos 1 mes de antelación, para permitir la planificación de las evaluaciones, indicando la fecha prevista.

6. En ambos casos (i. e ii.) ENAC realizará como mínimo un estudio de documentación del Plan de Transición de la entidad y su implantación, dotando a la evaluación de 1 jornada de tiempo adicional. La selección y propuesta de fechas deberá tener en cuenta lo dispuesto en el punto 8 de este Plan.

7. Una vez que su certificado de acreditación haga referencia a la nueva norma las entidades acreditadas dispondrán de dos meses de plazo (y siempre antes de **31.03.2026**) para empezar a llevar a cabo todas sus auditorías (iniciales, recertificación y seguimientos) con respecto a **ISO/IEC 27006-1:2024.**

8. Las desviaciones relativas a la acreditación en la nueva norma identificadas en las evaluaciones deberán ser adecuadamente respondidas por la entidad antes del **1 de febrero de 2026**. A partir de esta fecha, ENAC no puede garantizar que el resultado de la evaluación de las acciones correctivas recibidas se pueda presentar a Comisión de Acreditación antes de la fecha indicada en el punto 1 y, por tanto, las entidades que prevean su visita de evaluación próxima a esta fecha deberán asegurar un grado de implantación óptimo.

ANEXO I CAMBIOS RELEVANTES EN LA NUEVA VERSIÓN DE LA NORMA ISO/IEC 27006-1:2024

Esta identificación, realizada por IAF, no exime al certificador de hacer su propio análisis para identificar todos los cambios introducidos, de cara a adecuar su sistema de gestión a los nuevos requisitos.

A) Mejora de la redacción de los requisitos para las auditorías en remoto

1) nuevos requisitos para la realización de auditorías en remoto en 9.1.3.3;

2) el alcance y la eficacia de la utilización de la auditoría en remoto se indicarán en el informe de auditoría en 9.4.3.2;

3) eliminación de los requisitos para obtener la aprobación del organismo de acreditación si las actividades de auditoría en remoto representan más del 30% del tiempo previsto de auditoría in situ;

4) para el cliente con pocos o ningún emplazamiento físico relevante, el informe de auditoría (9.4.3.2) y el documento de certificación (8.2.2) deberán indicar que las actividades del cliente se realizan en remoto;

B) Actualización de los requisitos para el cálculo del tiempo de auditoría (Anexo C),

1) introduciendo el concepto de personas que realizan ciertas actividades idénticas en C.2.1 y la definición del requisito de como determinar el número inicial de personas en C.3.4, respectivamente;

2) nuevos requisitos sobre el tiempo de auditoría para las ampliaciones del alcance en C.7;

3) mayor claridad en el enfoque del cálculo del tiempo de auditoría de múltiples emplazamientos en C.6.

C) Actualización del Anexo D de ISO/IEC 27006:2015 para alinearlo con los controles de seguridad de la información enumerados en el Anexo A de ISO/IEC 27001:2022 y transfiriéndolo como Anexo E de ISO/IEC 27006-1:2024. La Tabla D ha sido renombrada como Tabla E;

D) Mejora de la redacción de los requisitos para hacer referencia a otras normas en los documentos de certificación del SGSI (8.2.3);

E) Eliminación de las redundancias con la norma ISO/IEC 17021-1:2015. Por ejemplo, se han actualizado las cláusulas 5.2, 7.1.3, 9.3.2.2 y 9.4 (ISO/IEC 27006-1:2024);

F) Eliminación del requisito cuantitativo de experiencia laboral y de formación requerido a los auditores del SGSI, por ejemplo, 4 años de experiencia práctica a tiempo completo;

ANEXO II ACCIONES DE LAS QUE DERIVA LA INFORMACIÓN A SOLICITAR POR PARTE DE ENAC PARA PREPARAR LA EVALUACIÓN

- Llevar a cabo una identificación y análisis de las diferencias entre las dos versiones de la norma

- Preparar un plan de transición que contemple:
    - Identificar los cambios entre versiones de norma. Los procesos afectados normalmente son ventas, ofertas, auditoria, gestión de la competencia, comunicación con clientes, etc.
    - Analizar el impacto de los cambios en las actividades y procesos relevantes e identificar las acciones necesarias para asegurar la conformidad (p.e. elementos o documentos del sistema de gestión, herramientas de TI)
    - Implementar las acciones requeridas.

- Asegurar que el personal relevante afectado por los cambios es competente para la nueva versión y para el proceso de transición. Dicho personal puede incluir, pero no se limita, a auditores, revisores, decisores, revisores de solicitud/contrato.

NOTA 1: Se requiere a las EC que planifiquen y comiencen las acciones necesarias tan pronto como sea posible.

NOTA 2: Con respecto a las organizaciones ya certificadas, como los requisitos sobre tiempo de auditoria han cambiado con la nueva versión de ISO/IEC 27006-1:2024, se hace notar que puede ser necesaria la actualización de los contratos entre EC y clientes a raíz de esos requisitos.