PLAN DE TRANSICIÓN DE ISO/IEC 27001:2013 A LA NUEVA ISO/IEC 27001:2022

Fecha de Emisión: **2022-03-01**

Dirigido a: Empresas titulares de la certificación ICONTEC de sistemas de gestión con la norma ISO 27001:2013.

Por medio de esta comunicación ICONTEC da a conocer el plan de transición que ha establecido ICONTEC para la norma **ISO 27001:2013** a la norma **ISO/IEC 27001:2022**

1. APROBACIÓN DE LA NUEVA NORMA ISO/IEC 27001:2022

El 25 de octubre de 2022 se publicó la nueva versión de la norma internacional ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información". Este documento proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de seguridad de la información y reemplaza la ISO/IEC 27001:2013.

Por otra parte, el pasado 9 de agosto de 2022 el Foro Internacional de Acreditación – IAF publicó el documento mandatorio IAF MD 26:2022 "TRANSITION REQUIREMENTS FOR ISO/IEC 27001:2022", el cual establece un periodo de transición de tres (3) años finalizando el 24 de octubre de 2025.

2. PRINCIPALES CAMBIOS DE LA NORMA ISO/IEC 27001:2022 FRENTE A LA NORMA ISO ISO/IEC 27001:2022

- En el numeral 4.2, se incluye el literal c, para que se identifiquen cuáles requisitos serán abordados a través de la gestión del sistema de seguridad de la información

- En el numeral 4.4, se incluyen las palabras en negrilla:

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

- En el numeral 5.1 “Liderazgo y Compromiso”, se incluye una nota referente a la interpretación de la palabra “negocios”:
La referencia a “negocios” en este documento puede interpretarse en sentido amplio para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

- En el numeral 6.2 “Objetivos de Seguridad de la Información y planificación para alcanzarlos”, se incluyen como requisitos los literales c y g:

c) Ser monitoreado
g) Estar disponible como información documentada

- Se incluyó como requisito el numeral 6.3 “planificación de cambios”

- En el numeral 7.4 “Comunicación”, se eliminaron los literales d y e:
d) quién hará la comunicación; y
e) Los procesos mediante los cuales se efectuará la comunicación

- En el numeral 8.1 “Planificación y control operativo” Se incluyen dos viñetas con mecanismos para la implementación de lo establecido en la cláusula 6, las cuales indican:
- establecer criterios para los procesos;
- implementar el control de los procesos de acuerdo con los criterios.

- En el requisito 9.3 “Revisión por la dirección”, se incluyen los numeral 9.3.1, 9.3.2 y 9.3.3, esta información antes se encontraba incluida en el numeral 9.3. En el numeral 9.3.2 se incluye el literal c) los cambios en las necesidades y expectativas de las partes interesadas, que sean pertinentes para el sistema de gestión de seguridad de la información.

- El nombre del Anexo A (Normativo) Objetivos de control y controles de referencia, se cambia por Anexo A (Normativo) ”Referencia de controles de seguridad de la información”. Además, los controles se alinean con ISO/IEC 27002:2022.

➢ En el anexo A (normativo), el número de controles en la ISO/IEC 27002:2022 disminuyó de 114 controles en 14 numerales a 93 controles en 4 numerales. Para los controles en la ISO/IEC 27002:2022, 11 de estos son nuevos, 24 migraron de los controles existentes y 58 fueron actualizados. Adicionalmente, se revisa la estructura de los controles, donde se introduce el "atributo" y "propósito" para cada uno de los estos y se elimina el uso de "objetivo" para un grupo de controles.

3. TRANSICIÓN DE LOS CERTIFICADOS VIGENTES OTORGADOS CON LA NORMA ISO/IEC 27001:2022

ICONTEC ha establecido un periodo de transición de tres (3) años a partir de la fecha de publicación de la norma ISO/IEC 27001:2022 (25 de octubre de 2022), por tanto, los certificados de ISO/IEC 27001:2013 no serán válidos a partir del 25 de octubre de 2025.

4. RECOMENDACIONES PARA LAS ORGANIZACIONES CON CERTIFICACIÓN DE SU SISTEMA DE GESTIÓN DE SEGURIDAD CON LA NORMA ISO/IEC 27001:2022

Para las organizaciones titulares de la certificación ICONTEC de su sistema de gestión con la norma ISO/IEC 27001:2013, se recomienda tener presente las siguientes directrices para actualizar exitosamente el sistema de gestión y por ende su certificación:

- Conocer los requisitos y conceptos de la norma revisada ISO/IEC 27001:2022.
- Identificar brechas organizacionales que se necesitan abordar para cumplir los requisitos nuevos o modificados.
- Definir y desarrollar un plan de transición para la actualización del sistema de gestión y la certificación a los nuevos requisitos, que incluya actividades, responsables en la organización, temas clave, los recursos requeridos y el cronograma de ejecución.
- Suministrar el entrenamiento y conocimiento apropiado a todas las partes que tienen un impacto en la eficacia y desempeño de la organización, en los nuevos requisitos y en el resultado esperado de su implementación.
- Actualizar la declaración de aplicabilidad (SoA).
- Identificar los nuevos controles o controles modificados por los clientes.
- Actualizar el plan de tratamiento de riesgos.
- Implementar, revisar y verificar la eficacia del nuevo plan de control de riesgos.

- Actualizar el sistema de gestión para cumplir los requisitos revisados y proporcionar la verificación de la eficacia.
- Verificar periódicamente el avance y la eficacia del plan de transición.
- Programar, planificar y ejecutar la auditoría interna al sistema de gestión, considerando los requisitos de la norma en general, considerando los requisitos nuevos y modificados.
- Definir e implementar las correcciones y acciones correctivas pertinentes.
- Realizar la revisión del sistema de gestión por la alta dirección de la organización.
- Coordinar y confirmar con ICONTEC el desarrollo de la auditoría de actualización.

5. OPCIONES PARA REALIZAR LA AUDITORÍA DE ACTUALIZACIÓN DE LA CERTIFICACIÓN CON LA NORMA ISO/IEC 27001:2022

ICONTEC ofrece a sus clientes certificados con ISO/IEC 27001:2013 la transición a la norma ISO/IEC 27001:2022, desde el 1 de julio de 2023 y presenta las siguientes opciones para su realización:

5.1 Alternativa A: Actualización de la certificación con la nueva versión en la auditoría de renovación del certificado con norma ISO/IEC 27001:2022 dentro del periodo correspondiente al ciclo de certificación actual de la organización y hasta cuatro (4) meses antes de la fecha límite para realizar la auditoría el 25 de junio de 2025.

5.2 Alternativa B: Actualización de la certificación mediante renovación anticipada con la norma ISO/IEC 27001:2022 en fecha anterior al próximo vencimiento de su certificado y hasta cuatro (4) meses antes de la fecha límite para la transición (25 de junio de 2025).

La duración de la auditoría que se realice bajo las alternativas A y B no requiere tiempo adicional al definido para la auditoría de renovación que ha sido determinado por en la propuesta comercial. Una vez se haya realizado la auditoría de actualización mediante renovación, con resultados satisfactorios y de acuerdo con lo establecido en el Reglamento de la Certificación R-PS-007, se procederá a actualizar el certificado con la versión 2022 de la norma respectiva, modificando las fechas del ciclo para iniciar un nuevo ciclo de certificación.

5.3 Alternativa C: Actualización de la certificación con la nueva versión ISO/IEC 27001:2022 en auditoría de seguimiento, dentro del periodo correspondiente al ciclo de certificación actual de la organización y hasta cuatro (4) meses antes de la fecha límite para la transición (25 de junio de

2025). Para esta Alternativa, ICONTEC incluirá en dicho seguimiento la evaluación de la conformidad de los requisitos nuevos y modificados en la norma ISO/IEC 27001:2022.

En todos los casos ICONTEC aumentará en 0.5 días el tiempo de la auditoria, por lo cual, la facturación del servicio para el año 2023 incluirá este tiempo adicional por única vez.

Una vez se haya realizado la auditoría de actualización, con resultados satisfactorios y de acuerdo con lo establecido en el Reglamento de la Certificación R-PS-007, se procederá a actualizar el certificado con la versión 2022 de la norma, sin modificar las fechas del ciclo de certificación.

5.4 Alternativa D: Actualización de la certificación mediante una auditoría independiente (extraordinaria) conservando el ciclo de certificación actual, es decir en una auditoría adicional a las establecidas en el ciclo del certificado.

La duración de la auditoría que se realice bajo la alternativa D será determinada tomando como punto de partida el cálculo del tiempo correspondiente a una auditoría de seguimiento y se aumentará en 0.5 días.

6. CERTIFICADOS DE SISTEMA DE GESTIÓN SUSPENDIDOS

En caso de que el certificado ICONTEC de sistema de gestión ISO/IEC 27001:2013 se encuentre suspendido durante la vigencia del plan de transición, el titular de la certificación podrá solicitar la auditoría de reactivación con la auditoría de seguimiento correspondiente y la auditoría de actualización de la certificación de manera conjunta, tomando como punto de partida el cálculo del tiempo correspondiente a una auditoría de seguimiento y se aumentará en 0.5 días. Si la suspensión se presenta en la segunda auditoria de seguimiento y la auditoría de reactivación se proyecta para ser realizada en una fecha cercana al vencimiento del certificado, el caso será revisado de manera particular por la Unidad técnica de Certificación.

7. OTROS LINEAMIENTOS ESTABLECIDOS POR ICONTEC

- Los servicios que se coticen para otorgamiento con la norma ISO/IEC 27001:2013 tiene como fecha máxima 25 de junio de 2024 para que sean prestados en esta versión, posterior a esta fecha todos los servicios deben ser prestados con la norma ISO/IEC 27001:2022.

- Las auditorias de actualización deberán ejecutarse antes del 25 de junio de 2025, con el fin de que el proceso finalice antes del 25 de octubre de 2025.

- Las auditorias de renovación que entren en proceso de restauración deben haber finalizado la totalidad de actividades pendientes incluidas la toma de decisión y ratificación por parte del Concejo Directivo antes del 25 de octubre de 2025.

- Las evaluaciones complementarias que se programen en la finalización del periodo de transición podrán tener como fecha máxima de realización 1 de septiembre de 2025.

- Los certificados de las organizaciones que no cumplan con los plazos establecidos para realizar la actualización a la nueva versión de la ISO/IEC 27001:2022 pasaran a estado de cancelación siendo necesario iniciar un nuevo proceso de otorgamiento.

- Para las opciones indicadas en los numerales 5.1 a 5.4, una vez se haya realizado la auditoría de actualización, con resultados satisfactorios y de acuerdo con lo establecido en el Reglamento de la Certificación R-PS-007, se procederá a actualizar el certificado con la versión 2022 de la norma, sin modificar las fechas del ciclo de certificación.

- Estos certificados serán emitidos inicialmente sin logo de acreditación, una vez ONAC confirme la actualización de la acreditación de ICONTEC a la ISO/IEC 27001:2022, los certificados serán actualizados con el respectivo logo símbolo de la acreditación en la siguiente auditoria del ciclo de certificación.

Cordialmente,

Fabian Leonardo Colorado Abella
Gerente de certificación - ICONTEC