OCA GLOBAL

ISO/IEC 27001 VERSIÓN 2022

(seguridad de la información, ciberseguridad y protección de la privacidad)

Certificación


Performance
Video
3D Data
Released
Speed
Architecture
Data
Performance
Data
3D Data
Architecture
Released
Video
3D Data
Data
Product
Performance
Data
Features
Released
PCIe
Work
Workstation
Video
Data
Loading
Workstation
Video
3D Data

PLAZOS DE TRANSICIÓN PARA SU ADECUACIÓN, MEJORAS Y NOVEDADES

¿EL PORQUÉ DE SU ACTUALIZACIÓN?

Periódicamente, todas las normas ISO se revisan, un requisito imprescindible para mantener las normas de gestión de la información al día y, sobre todo, con el panorama de la ciberseguridad en constante evolución. Ello se intensifica a partir de la pandemia. Desde entonces se han aceptado nuevas maneras de trabajar las cuales han tenido un impacto positivo gracias al trabajo remoto y la democratización de la nube.

Así, el **25 de octubre de 2022** se actualizó la norma ISO 27001 a su **versión 2022**.

¿CUÁLES SON LAS MOTIVACIONES PARA SU ACTUALIZACIÓN?

La creciente digitalización de las empresas de diferentes sectores, en las que se ha tomado esta norma como columna vertebral para la gobernanza TI, ha conllevado esta actualización. Entre los principales motivos más relevantes:

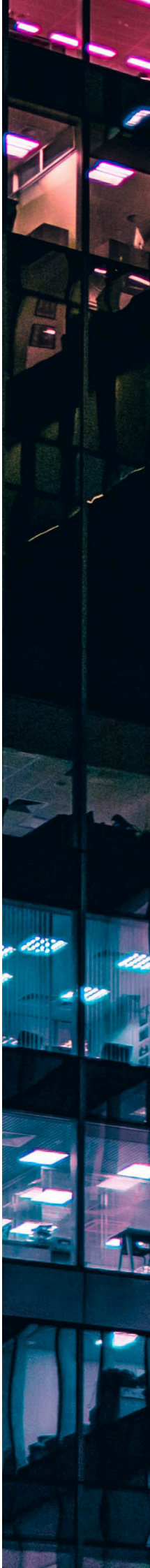
- Los nuevos riesgos de seguridad han obligado la obtención de mejoras en ISO, tanto en el ámbito de categorización como en el de la gestión de los controles de seguridad.
- Desde 2013, ha habido cambios en cuanto a la documentación para la protección de datos personales.
- La actualización de 27002 a su versión 2022, de la cual ISO 27001 utiliza controles para su Anexo A.

¿QUÉ OBJETIVOS PERSIGUE ISO 27001 VERSIÓN 2022?

La actualización de ISO 27001:2022, no pretende hacer cambios disruptivos. Tiene un carácter más continuista, pero actualizado. Estas actualizaciones se centran en:

- Alinear ISO 27001 con una respuesta más precisa contra las vulnerabilidades, también considerando que la guía ISO 27002:2022 representa los controles de seguridad de la información, cuya actualización se integra para atender y responder a estos nuevos escenarios

- Reforzar la protección frente a las nuevas tendencias de ciberseguridad, más ahora que la red empresarial se ha extendido a los hogares de los empleados, reduciendo vulnerabilidades y promoviendo la vigilancia continua.

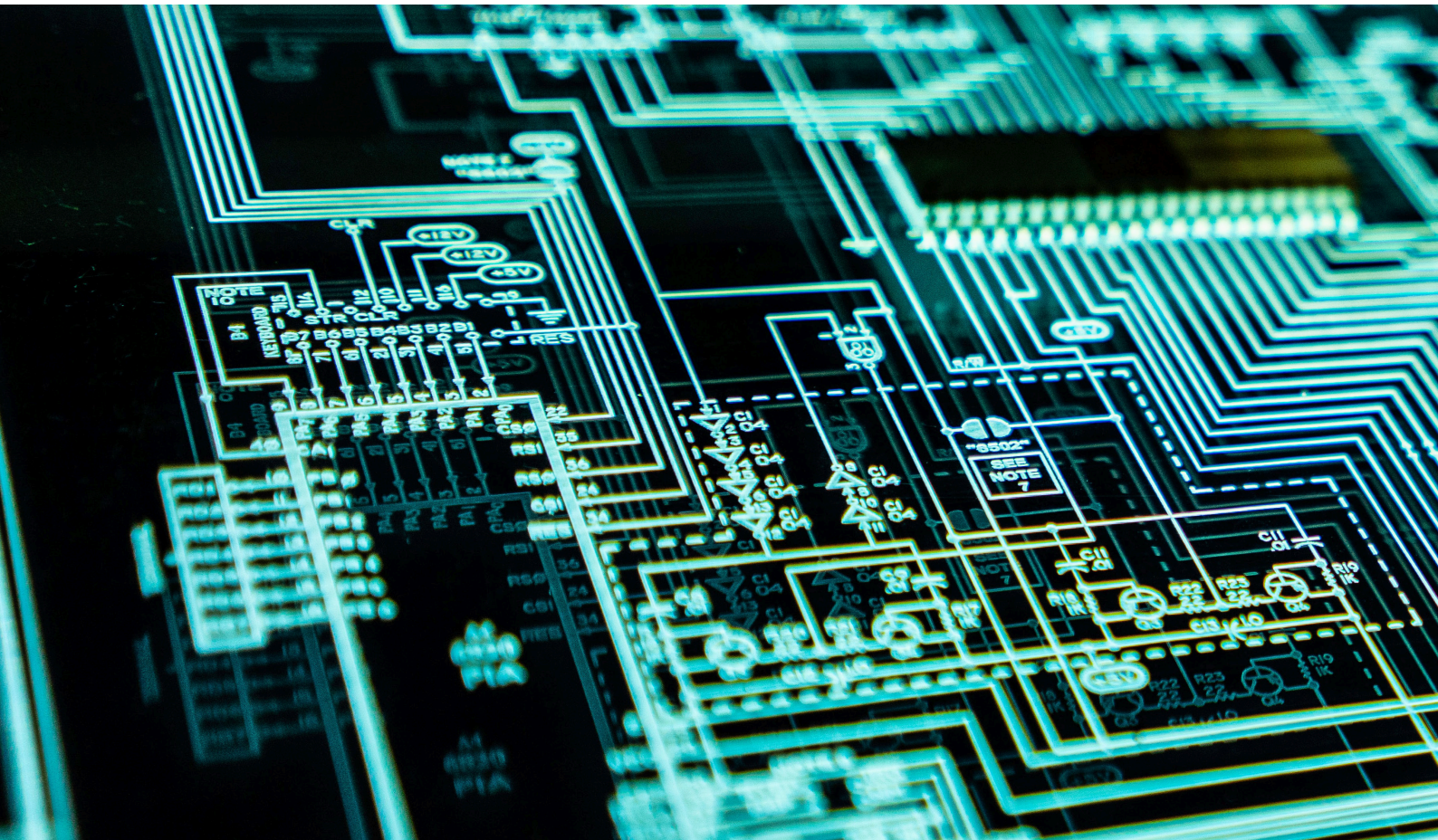


PRINCIPALES ACTUALIZACIONES EN ISO 27001:2022

Los cambios en su cuerpo no han sido significativos, se han actualizado varios apartados y otros no han sufrido algunas variaciones:

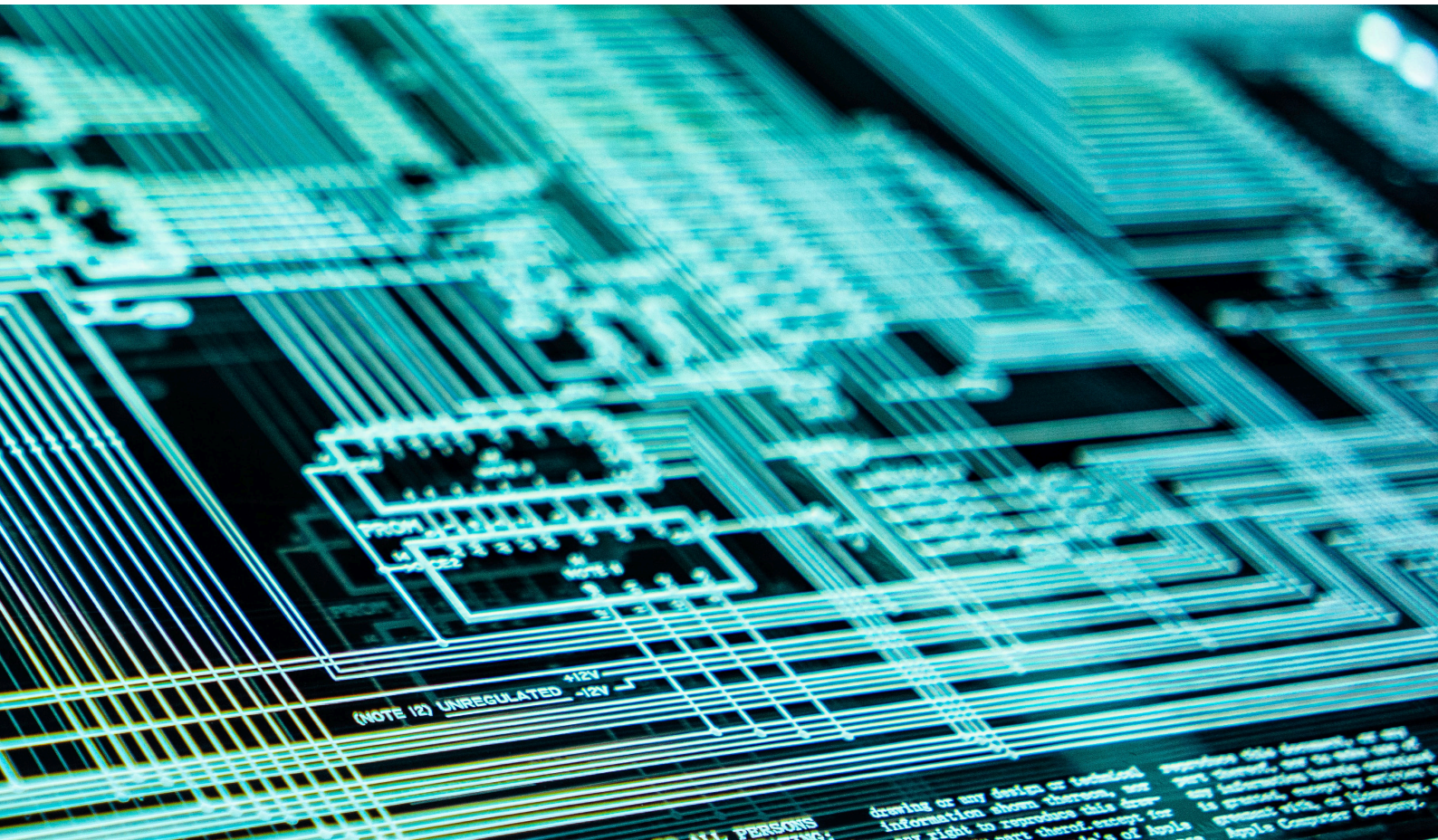
1. En cuanto a la estructura de alto nivel (Anexo SL), las cláusulas del 4 al 10 no han tenido variación alguna.

ANEXO SL ESTRUCTURA DE ALTO NIVEL	CLAUSULAS DEL ANEXO SL QUE NO VARIAN EN ISO 27001:2022
1. Alcance 2. Referencias Normativas 3. Términos y definiciones 4. Contexto de la organización 5. Liderazgo 6. Planificación 7. Soporte 8. Operación 9. Evaluación del desempeño 10. Mejora	4. Contexto de la organización 5. Liderazgo 6. Planificación 7. Soporte 8. Operación 9. Evaluación del desempeño 10. Mejora



2. Su mayor actualización ha sido sobre el Anexo A (ISO 27002:2022), donde la versión anterior estaba conformada con 114 controles de seguridad. Con esta actualización, ahora solo son 93 controles, en los cuales ha habido una reestructuración, racionalización y reagrupación de controles con el objetivo de minimizar los controles y agruparlos de una manera más lógica y de fácil entendimiento.

ANEXO A: ISO 27001: 2017	**Anexo A: ISO 27001: 2022**
14 dominios,114 controles	**4 dominios, 93 controles**
*A.5 Políticas de Seguridad de la Información *A.6 Organización de la Seguridad de la Información *A.7 Seguridad relativa a los recursos humanos *A.8 Gestión de Activos *A.9 control de Acceso *A.10 Criptografía *A.11 Seguridad Física y del entorno *A.12 Seguridad de las operaciones	*A.5 Controles Organizacionales *A.6 Controles de Personas *A.7 Controles Físicos *A.8 Controles Tecnológicos



Además, hay un total de 11 nuevos controles, 24 se han fusionado, 58 han sido revisados y 35 no han sufrido ningún cambio.

Los controles en el Anexo A actualizado están estructurados de la siguiente manera:

Controles organizacionales: 37 controles, de los cuales 34 son preexistentes y 3 nuevos.

5. CONTROLES ORGANIZACIONALES

5.1. Políticas de seguridad de la información
5.2. Roles y responsabilidades de seguridad de la información
5.3. Segregación de deberes
5.4. Responsabilidades de gestión
5.5. Contacto con autoridades
5.6. Contacto con grupos de interés especial

5.7. Inteligencia de amenazas

5.8. Seguridad de la información en la gestión de proyectos.
5.9. Inventario de información y otros activos asociados
5.10. Uso aceptable de la información y otros activos asociados
5.11. Devolución de activos
5.12. Clasificación de la información
5.13. Etiquetado de información
5.14. Transferencia de información
5.15. Control de acceso
5.16. Gestión de identidad
5.17. Información de autenticación
5.18. Derechos de acceso
5.19. Seguridad de la información en las relaciones con los proveedores
5.20. Abordar la seguridad de la información en los acuerdos con los proveedores
5.21. Gestión de la seguridad de la información en la cadena de suministro de las TIC
5.22. Seguimiento, revisión y gestión de cambios de servicios de proveedores

5.23. Seguridad de la Información para el uso de servicios en l a nube.

5.24. Planificación y gestión de incidentes de seguridad de la información.
preparación
5.25. Evaluación y decisión sobre eventos de seguridad de la información
5.26. Respuesta a incidentes de seguridad de la información
5.27. Aprender de los incidentes de seguridad de la información
5.28. Recolección de evidencia
5.29. Seguridad de la información durante la interrupción

5.30. Preparación de las TIC para la continuidad del negocio.

5.31. Requisitos legales, estatutarios, reglamentarios y contractuales
5.32. Derechos de propiedad intelectual
5.33. Protección de registros
5.34. Privacidad y protección de PII
5.35. Revisión independiente de la seguridad de la información.
5.36. Cumplimiento de políticas, normas y estándares de información seguridad
5.37. Procedimientos operativos documentados

Controles de personas: 8 controles, todos preexistentes.

6. CONTROLES DE PERSONAS

6.1. Poner en pantalla
6.2. Términos y condiciones de empleo
6.3. Concientización, educación y capacitación en seguridad de la información
6.4. Proceso Disciplinario
6.5. Responsabilidades después de la terminación o cambio de empleo
6.6. Acuerdos de confidencialidad o no divulgación
6.7. Trabajo remoto
6.8. Informes de eventos de seguridad de la información

Controles físicos: 14 controles, 13 preexistentes y 1 nuevo.

7. CONTROLES FÍSICOS

7.1. Perímetro de seguridad física
7.2. Entrada física
7.3. Asegurar oficinas, salas e instalaciones

7.4. Monitoreo de seguridad física

7.5. Protección contra amenazas físicas y ambientales.
7.6. Trabajar en áreas seguras
7.7. Cleardeskandclearscreen
7.8. Ubicación y protección de equipos
7.9. Seguridad de los activos fuera de las instalaciones
7.10. Medios de almacenamiento
7.11. Utilidades de apoyo
7.12. Seguridad del cableado
7.13. Mantenimiento de equipo
7.14. Eliminación segura o reutilización de equipos

Controles tecnológicos: 34 controles, 27 controles preexistentes y 7 nuevos.

8. CONTROLES TECNÓLOGICOS

8.1. Dispositivos de punto final de usuario
8.2. Derechos de acceso privilegiado
8.3. Restricción de acceso a la información
8.4. Acceso al código fuente
8.5. Autenticación segura
8.6. Gestión de capacidad
8.7. Protección contra malware
8.8. Gestión de vulnerabilidades técnicas

8.9. Gestión de la configuración
8.10. Eliminación de la información
8.11. Enmascaramiento de datos
8.12. Prevención de fuga de datos

8.13. Copia de seguridad de la información
8.14. Redundancia de las instalaciones de procesamiento de información
8.15. Inicio sesión

8.16. Actividades de seguimiento

8.17. Sincronización de reloj
8.18. Uso de programas de utilidad privilegiados
8.19. Instalación de software en sistemas operativos
8.20. Seguridad de la red
8.21. Seguridad de los servicios de red.
8.22. Segregación de redes

8.23. Filtrado WEB

8.24. Uso de criptografía
8.25. Ciclo de vida de desarrollo seguro
8.26. Requisitos de seguridad de la aplicación
8.27. Arquitectura e ingeniería de sistemas seguros principios

8.28. Codificación segura

8.29. Pruebas de seguridad en desarrollo y aceptación
8.30. Desarrollo subcontratado
8.31. Separación de desarrollo, prueba y producción ambientes
8.32. Gestión del cambio
8.33. Información de prueba
8.34. Protección de los sistemas de información durante la auditoría pruebas

3. ISO 27002:2022, dispone de 5 atributos que pueden ayudar de forma significativa en la categorización, así como en su monitoreo.

- Tipo de Control: este evalúa cómo y cuándo el control puede modificar el riesgo, con respecto a la ocurrencia de un incidente. Puede clasificarse en: preventivos, correctivos y predictivos.

- Propiedades de la seguridad de la información: identifica qué características de la información contribuyen a preservar el control. Pueden ser: confidencialidad, integridad y disponibilidad.

- Conceptos de Ciberseguridad: establece una relación entre los controles y los conceptos de ciberseguridad, los cuales son descritos en la ISO 27110: identificar, proteger, detectar, responder y recuperar.

- Capacidad operativa: atributo con el cual se pueden ver los controles desde la perspectiva del encargado de la seguridad de la información: gobernanza, gestión de activos, protección de la información.

- Dominios de seguridad: atributo que permite visualizar a los controles desde el punto de vista de cuatro dominios de seguridad: gobernanza, protección, defensa y resiliencia.

ATRIBUTOS ISO 27002

1. Tipo de Control
2. Propiedades de seguridad de la información
3. Conceptos de Ciberseguridad.
4. Capacidades Operativas.
5. Dominios de Seguridad

AUDITORÍA DE TRANSICIÓN DE 27001:2017 HACIA ISO 27001:2022

Cuando se requiera una auditoría para certificarse en la nueva versión de ISO 27001, será necesario enfocarse en varios apartados:

- Analizar las brechas de seguridad de ISO 27001:2022 y la necesidad de cambios en el SGSI del cliente, si fuera necesario.
- La actualización de la declaración de aplicabilidad (S.O.A).
- La actualización del plan de tratamiento de riesgos, si fuera necesario.
- La implementación y la comprobación de la eficacia de los nuevos controles, así como las modificaciones llevadas a cabo por el cliente.

¿QUÉ PLAZO TENGO PARA LA TRANSICIÓN?

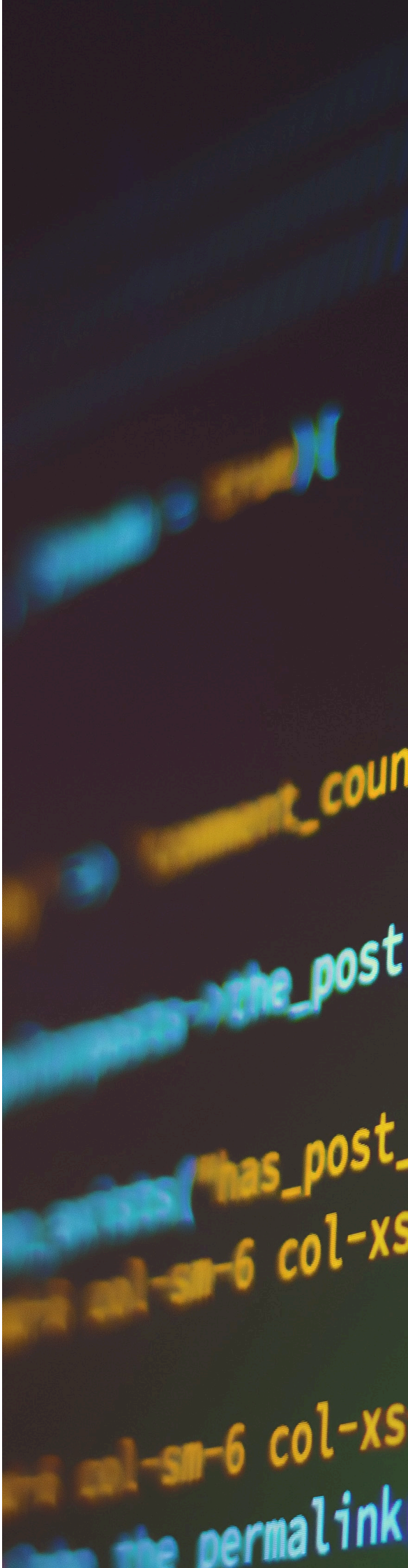
Desde el momento de publicación de la norma ISO 27001:2022, se iniciará un plan de transición de 3 años (36 meses), en el cual las organizaciones deberán adaptar sus sistemas a las actualizaciones introducidas.

¿CUÁL ES LA FECHA DE CADUCIDAD DE LA NORMA ISO 27001:2017?

ISO 27001:2017, seguirá teniendo vigencia hasta el **25/10/2025**. Es decir, las organizaciones que estén en proceso de implantación de sus sistemas y se certifiquen en base a ISO 27001:2017, la vigencia máxima de estos certificados será hasta el **25/10/2025**.

¿QUÉ PASA SI YA ESTOY EN UN PROCESO DE CERTIFICACIÓN?

En los procesos de certificación ya iniciados, o que se encuentren en cualquier fase de auditoría, se mantendrán los procesos en curso bajo ISO 27001:2017 y la validez de estos certificados será hasta el **25/10/2025**.



¿SI YA TENGO UN CONTRATO CON OCA CERT, QUÉ TENGO QUE HACER PARA ADECUARLO A LA NUEVA NORMA?

Recordad que no hay apremio. Hay un periodo de transición de tres años. Una vez que se tenga implantado el sistema con la nueva norma, debes solicitar la adecuación de tu contrato y servicio a la nueva norma, a través de nuestra red de comerciales.

En el caso de que no se haya llevado a cabo ninguna fase del proceso de certificación por nuestra parte, tras su petición se hará una revisión de contrato de servicio para adecuarlo a la nueva norma.

En caso de tener avanzado el proceso de certificación o que tengas ya certificado tu sistema con la antigua norma, puedes:

- **Continuar como estaba previsto.** Todavía tienes un total de tres años para la transición a la nueva norma.
- **Solicitar la adaptación de la nueva norma en el seguimiento anual de la certificación.** Para la adaptación, es obligatorio que se lleve a cabo una solicitud previa a la planificación de la misma, para garantizar la disponibilidad de fechas y recursos y poder llevar a cabo la adaptación en las fechas solicitadas. En el caso de adaptación en seguimiento, los tiempos mínimos necesarios para la transición son de 1 jornada
- **Solicitar la adaptación en la renovación de la certificación.** Es obligatorio que para la adaptación se lleve a cabo una solicitud previa a la planificación de la misma, para garantizar la disponibilidad de fechas y recursos para poder llevar a cabo la adaptación en la fecha solicitada. En el caso de adaptación en renovación, los tiempos mínimos necesarios para la transión son de 0,5 jornadas.

- **En cualquier momento, solicitar la adaptación del certificado en vigor ISO 27001:2017 a la nueva norma**, donde se evaluará el cumplimiento de la misma mediante una auditoría extraordinaria. En el caso de adaptación a traves de auditoria extraordina, los tiempos mínimos necesarios para la transión son de 1 jornada.
- **Transferencia de certificados.** La transferencia de los certificados se llevará a cabo con la misma norma de la Entidad de Certificación de origen. Para la transferencia de las nuevas normas, se tendrán en cuenta las acreditaciones de la Entidad de Certificación de origen y OCA CERT.

En cualquier caso, para emitir un certificado de acuerdo con la nueva versión de las normas será necesario auditar el sistema de gestión, de acuerdo a los nuevos requisitos.

OCA
GLOBAL

www.ocaglobal.com