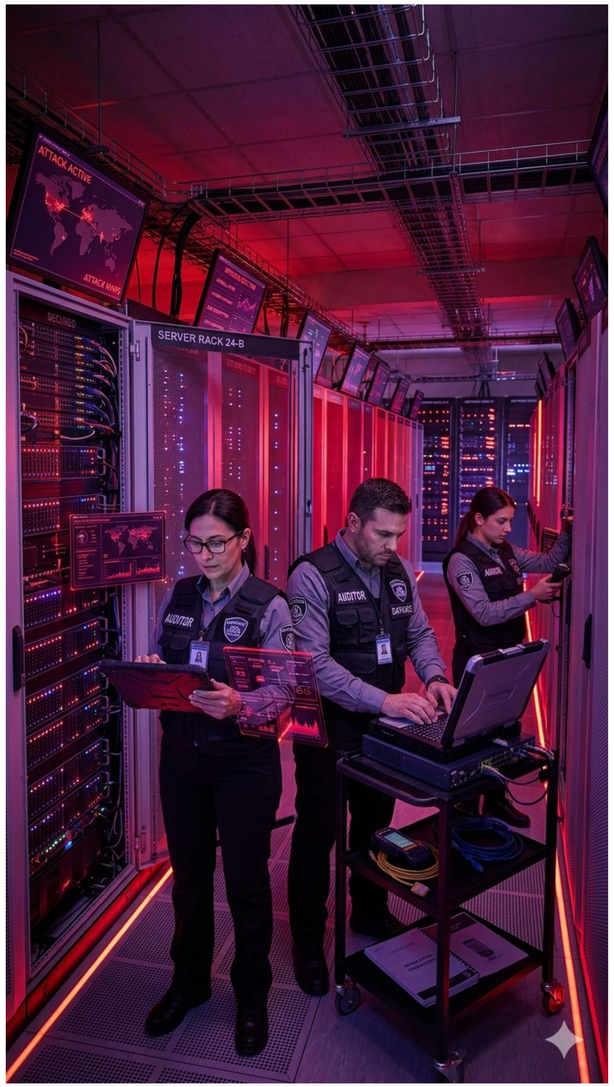
CHIEF AUDITOR ISO IEC 27001:2022
Training Material



Tactical Compliance Badges

Idioma: Español
Ver:2026
Creado por: Valfra It Consulting.

Módulo B ISO IEC 27006-1:2022

Quien es Valfra It Consulting

Empresa 100% mexicana, fundada en 2009.

Somos el mejor equipo de profesionales creando un concepto innovador en servicios de consultoría, auditoría, capacitación y certificación, buscando reunir el mejor talento de profesionales para ofrecer servicios de excelencia en las mejores prácticas y sistemas de gestión en México, Canadá, EUA y Latinoamérica.

Líderes en implementación de mejores prácticas y sistemas de gestión, somos asesores reconocidos gracias a la calidad de nuestro servicio.

Miembros de la red de empresas Dun & Bradstreet somos reconocidos internacionalmente por las organizaciones fijadoras de estándares con mayor influencia del mundo, más de 50 asociaciones comerciales e industriales, el Gobierno Federal de Estados Unidos y las Naciones Unidas, entre otras instituciones.

Diamond partners de CERTIPROF LLC® organismo internacional para evaluar y certificar competencias a nivel mundial; VALFRA IT CONSULTING ha capacitado y certificado a cientos de profesionistas en normas internacionales como ISO 27001, ISO 22301, ISO 20000, ISO 9000 y mejores prácticas como Ciberseguridad, ITIL, SCRUM, NIST y NICE.

Valor y Experiencia

Con 17 años de experiencia hemos desarrollado, compartido conocimiento y experiencias en cuanto al conjunto de las prácticas más actuales, con la finalidad que las TI cumplan su propósito y objetivo.

Nuestra misión

Convertirnos en su socio de negocio y aliado estratégico.

Nuestras Afiliaciones

certiprof®

Badge Digital

Los Badges digitales contienen información sobre quién las ha obtenido, las competencias requeridas y la organización que las ha expedido. Algunas insignias incluso están vinculadas a las actividades necesarias para obtenerlas.

Permiten a los profesionales mostrar y verificar sus logros de manera instantánea y global, los perfiles de LinkedIn con insignias digitales reciben más atención por parte de reclutadores y empleadores.

Se reportó que esto mejoró su credibilidad profesional en sus redes. Además, que los Badges digitales les ayudan a identificar rápidamente habilidades específicas.

Se ha demostrado que incluirlos en currículums genera más de probabilidades de contratación en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.

Badge Digital

Los Certificados de Cumplimiento Táctico

CHIEF AUDITOR 27001:2022

(Complemento de los Certificados Auditor Líder 27001:2022)

son indispensables para aquellas personas que quieran demostrar competencias en AUDITORÍAS EXTERNAS y ejercer como auditores de segunda o tercera parte **en Sistemas de Gestión de Seguridad de la Información (SGSI), en organismos auditores y/o de certificación** en apego a las normas **ISO/IEC 17021:2015 e ISO/IEC 27006:2022.**

Badge Digital

https://valfraitconsulting.com/registro-de-auditores

Requisitos de inscripción al registro de auditores

Certificado vigente de Auditor Líder y/o Auditor Interno emitido por CERTIPROF LLC® y/o VALFRA IT CONSULTING.

Certificado vigente de Jefe Auditor (Chief Auditor) emitido por CERTIPROF LLC® y/o VALFRA IT CONSULTING.

REGISTRO DE AUDITORES

La norma ISO/IEC 17021-1 exige a los Organismos de Certificación y/o Auditorías Externas mantener un registro de personal que avale las competencias de los auditores. Para tal finalidad, VALFRA IT CONSULTING cuenta con un registro actualizado de los Certificados de Cumplimiento Táctico CHIEF AUDITOR, el cual permite a los organismos de certificación y a las organizaciones auditadas validar las competencias y experiencia de un auditor.

Información que puede validar en nuestros registros:

Validez y vigencia del certificado.

Experiencia laboral en auditorías (auditorías reportadas).

Evidencia de evaluación de competencias solicitadas por la norma relacionada, tales como la ISO/IEC 27001:2022 o la ISO 22301:2019.

Resultado de evaluaciones reportadas al auditor.

📌 Auditores externos: El requisito aplica a los auditores subcontratados (auditorías de 2da. parte) o de certificación (auditorías de 3ra. parte).

Finalidad: Las entidades de acreditación (como ANAB en EE. UU. o la Entidad Mexicana de Acreditación en México) revisan estos registros documentados durante las auditorías de supervisión para verificar que la certificadora opera con personal calificado, de manera transparente y libre de conflictos de interés.

Introducción al curso

Estructura de la norma 17021-1:2015

El Rol Chief Auditor es un complemento al Rol Lead Auditor e Internal Auditor para desarrollar competencias en AUDITORÍAS EXTERNAS como auditores de segunda o tercera parte en apego a las normas 17021-1:2015 e **ISO/IEC 27006-1:2022**.

Introducción al curso

Estructura de la norma 17021-1:2015

ISO/IEC 17021-1:Establece los requisitos para los organismos que realizan la auditoría y certificación de sistemas de gestión.

Normas complementarias fundamentales son las de la serie ISO/IEC 17021.

Estas normas adicionales introducen los requisitos específicos de competencia para los auditores y el personal involucrado en el proceso de certificación, dependiendo del tipo de sistema de gestión que se esté evaluando.

- ISO/IEC TS 17021-2:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión Ambiental (SGA) (ISO 14001).
- ISO/IEC TS 17021-3:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión de la Calidad (ISO 9001).
- ISO/IEC TS 17021-4:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión de la Sostenibilidad de Eventos (ISO 20121).
- ISO/IEC TS 17021-5:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión de Activos (ISO 55001).
- ISO/IEC TS 17021-6:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión de la Continuidad del Negocio (SGCN) (ISO 22301).
- ISO/IEC TS 17021-7:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión de la Seguridad del Tráfico (ISO 39001).
- ISO/IEC TS 17021-9:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión Antisoborno (ISO 37001).
- ISO/IEC TS 17021-10:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión de la Seguridad y Salud en el Trabajo (SGSST) (ISO 45001).
- ISO/IEC TS 17021-11:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión para la Infraestructura y Equipamiento en Centros de Salud.
- ISO/IEC TS 17021-12:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión de la Relación de Negocios Colaborativa (ISO 44001).
- ISO/IEC TS 17021-13:Requisitos de competencia para la auditoría y la certificación de Sistemas de Gestión para el Cumplimiento (Compliance) (ISO 37301).

Introducción al curso

Estructura de la norma 17021-1:2015

El caso específico de Seguridad de la Información (ISO/IEC 27006-1:2022)

Es muy importante notar que para los Sistemas de Gestión de Seguridad de la Información (SGSI / ISO/IEC 27001:2022), el documento complementario no pertenece a la serie 17021, sino a la serie 27000:

ISO/IEC 27006-1:2022: Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión de la seguridad de la información. Este estándar actúa en conjunto con la ISO/IEC 17021-1:2015, añadiendo los requisitos específicos e indispensables para la auditoría de un SGSI, tales como la delimitación matemática del alcance de las TIC, el mapeo mandatorio de la Declaración de Aplicabilidad (SoA), y el registro explícito de su versión y fecha en los documentos de certificación.

Aunque no son extensiones directas de la 17021-1:2015, el ecosistema de evaluación de la conformidad se complementa fuertemente con:

ISO/IEC 17011:2017: Requisitos para los organismos de acreditación que acreditan a los organismos de evaluación de la conformidad (es la norma que utilizan entidades como la EMA en México para auditar a las casas certificadoras).

ISO/IEC 19011:2018: Directrices para la auditoría de los sistemas de gestión. Aunque la 17021-1:2015 define los requisitos legales y contractuales de la certificación, la 19011 proporciona la metodología práctica sobre cómo ejecutar cualquier auditoría interna o externa.

Nota de aplicación: Cuando un organismo de certificación busca la acreditación para un esquema específico (por ejemplo, ISO 27001:2022), debe demostrar el cumplimiento estricto de **ISO/IEC 17021-1:2015 + ISO/IEC 27006-1:2022**.

Norma 27006-1:2022

Norme internationale

ISO/IEC 27006-1

Première édition
2024-03

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information —

Partie 1:
Généralités

Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems —

Part 1: General

Numéro de référence
ISO/IEC 27006-1:2024(fr)

Estándar internacional que establece los requisitos para los organismos que realizan la auditoría y certificación de sistemas de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2022; Parte 1: "Generalidades" es la norma internacional que define las reglas de juego para las empresas que auditan y otorgan los certificados de ISO 27001.

🎯 Objetivo Principal: Garantizar que cuando una organización reciba un certificado ISO 27001, el mercado pueda confiar plenamente en que la auditoría fue rigurosa, transparente y ejecutada por personal altamente calificado. Actúa como un complemento específico de la norma general de acreditación ISO/IEC 17021-1.

Clausulado Norma 27006-1:2022

1. Objeto y campo de aplicación
2. Referencias normativas
3. Términos y definiciones

4. Principios generales
5. Requisitos generales
6. Requisitos estructurales
7. Requisitos para los recursos
8. Requisitos de información
9. Requisitos del proceso
10. Requisitos del sistema de gestión para los organismos de certificación

Nota: Estructura diseñada para acoplarse de forma exacta y como un "espejo" a la estructura de la norma madre de acreditación, la ISO/IEC 17021-1.

1. Objeto y campo de aplicación

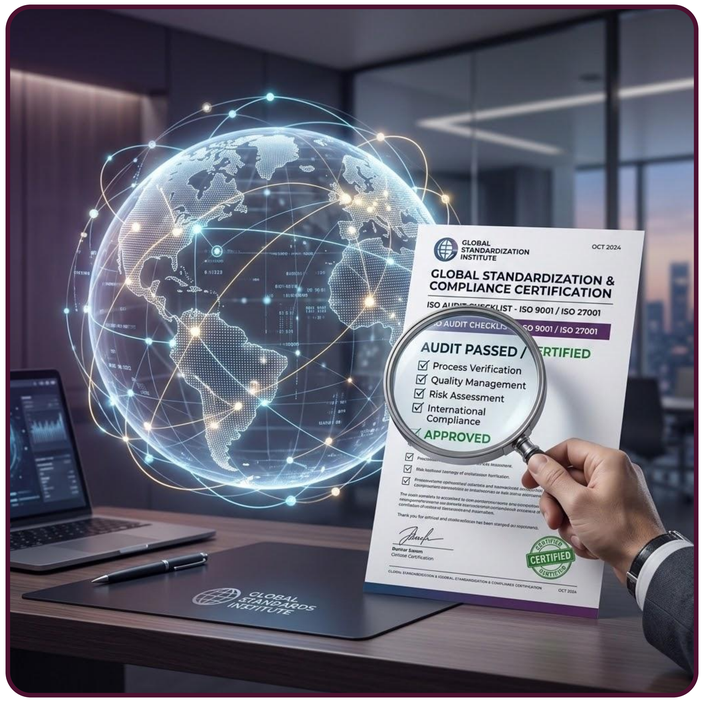
Este documento especifica los requisitos y proporciona orientación para los organismos que realizan la auditoría y la certificación de un sistema de gestión de la seguridad de la información (SGSI), **de forma adicional a los requisitos contenidos en la norma ISO/IEC 17021-1.**

Los requisitos contenidos en este documento son demostrados en términos de competencia y confiabilidad por los organismos que prestan la certificación de SGSI.

La orientación contenida en este documento proporciona una interpretación adicional de estos requisitos para los organismos que prestan la certificación de SGSI.

NOTA: Este documento puede utilizarse como un documento de criterios para la acreditación, la evaluación por pares u otros procesos de auditoría.

⚠️ Nota de Interpretación: El uso del término "debe" (shall) en este documento indica un requisito obligatorio que los organismos de certificación (Casas Certificadoras) tienen que aplicar para demostrar competencia, consistencia e imparcialidad.

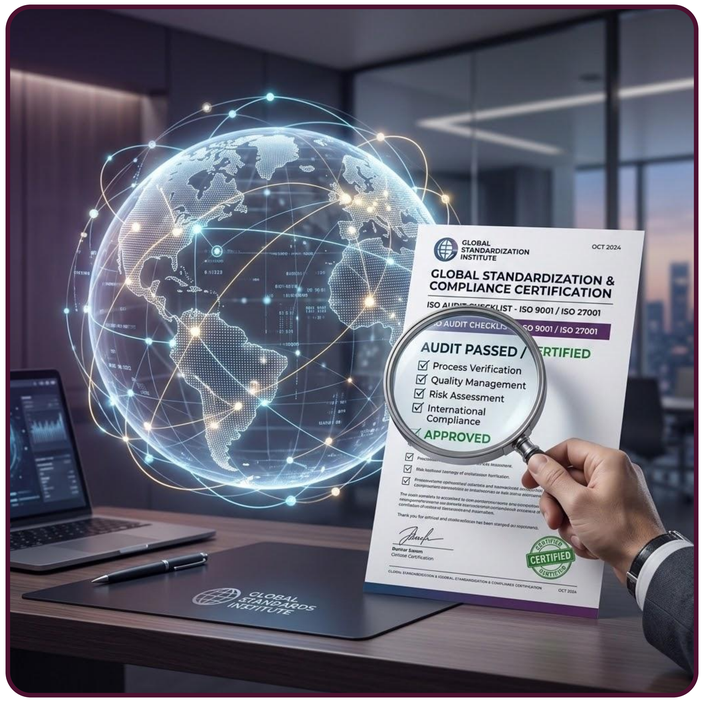


1. Objeto y campo de aplicación

- Para evitar interpretaciones erróneas en el mercado corporativo, la Cláusula 1 delimita estrictamente el uso de la norma:

- **No es una norma de implementación empresarial:** Este documento no establece requisitos para las organizaciones que implementan un SGSI para proteger sus datos corporativos (para eso existe la ISO/IEC 27001).

- **No aplica a auditorías internas:** Las directrices para realizar auditorías internas de primera o segunda parte quedan fuera de este documento y se rigen bajo la norma ISO 19011.



1. Objeto y campo de aplicación

📝 Directrices Clave de Aplicación Práctica (Derivadas de la Cláusula 1)

Para entender cómo se aterriza esta cláusula en el ecosistema de certificación, la norma establece que el "campo de aplicación" obliga a que la auditoría de certificación sea entendida bajo un marco de tres pilares interactivos:

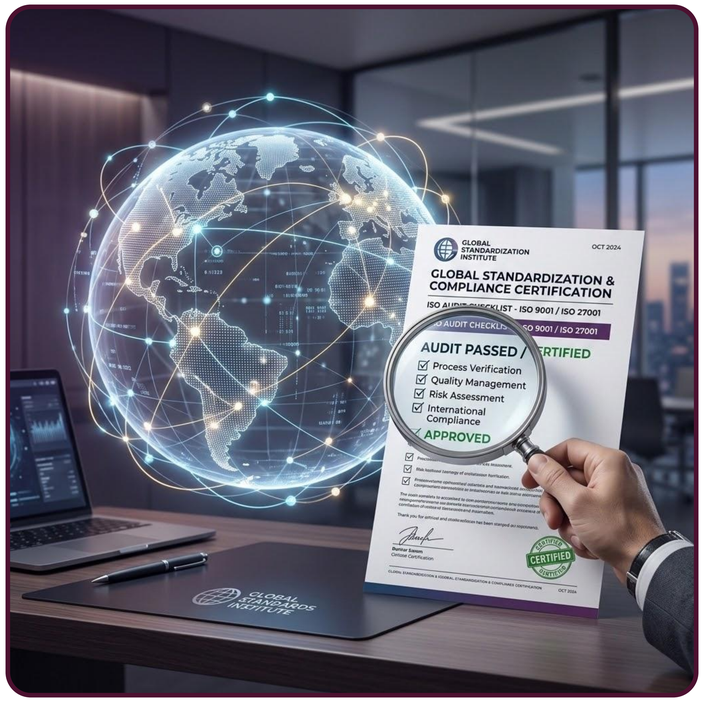
[ISO/IEC 17021-1] ----> Requisitos generales para auditorías de sistemas de gestión.

+

[ISO/IEC 27006-1] ----> Requisitos ESPECÍFICOS para Seguridad de la Información.

=

Auditoría Válida de la Norma ISO/IEC 27001



Criterio de Equivalencia: Las Entidades de Acreditación (como ENAC, EMA, UKAS, etc.) utilizarán este objeto y campo de aplicación como el checklist definitivo para evaluar y decidir si una Casa Certificadora está calificada o no para operar en el mercado de la ciberseguridad.

2. Referencias normativas

Los siguientes documentos son indispensables para la aplicación de este documento:

ISO/IEC 17021-1

Evaluación de la conformidad — Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.

ISO/IEC 27001

Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos.

3. Términos y definiciones

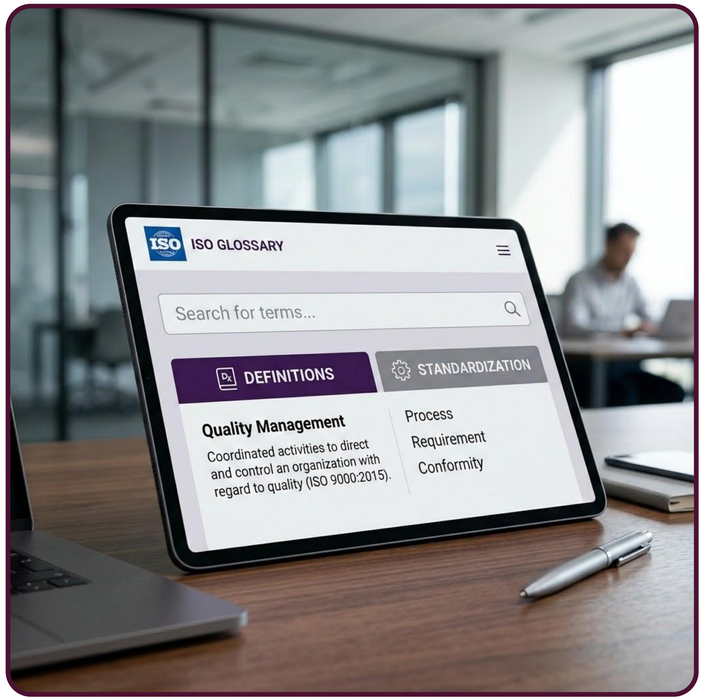
📋 Estructura de la Cláusula 3: Bases Conceptualización

💡 Para evitar duplicar texto innecesariamente, la norma establece en su introducción conceptual que, para los propósitos de este documento, s**e aplican los términos y definiciones incluidos en las siguientes normas madre:**

ISO/IEC 17021-1 (Conceptos de auditoría y certificación en general).

ISO/IEC 27000 (El glosario general para todos los estándares de la familia de seguridad de la información).

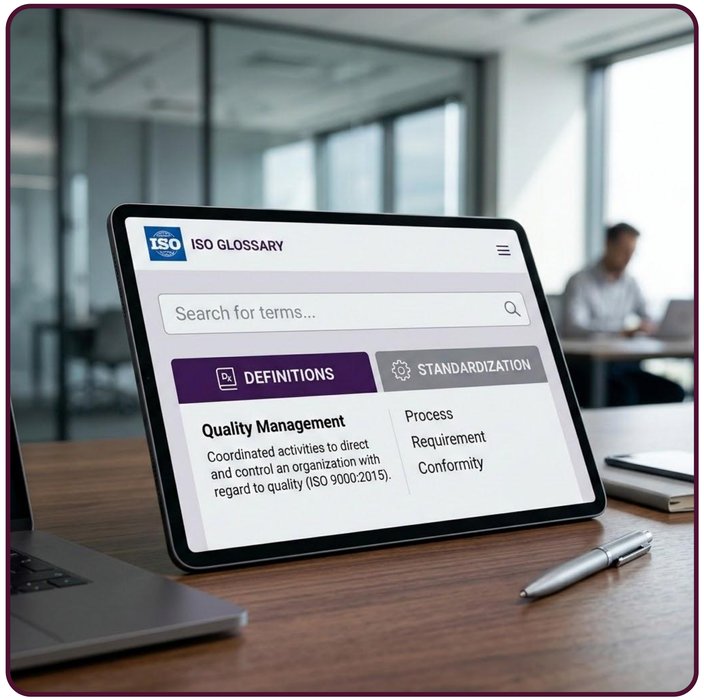
Sin embargo, la norma procede a detallar o enfatizar definiciones específicas que son críticas para el proceso de certificación de un SGSI.



3. Términos y definiciones

🔍 Conceptos Clave y Definiciones Destacadas

Aunque la norma se apoya en los glosarios madre, el enfoque de la Cláusula 3 resalta y delimita términos críticos como los siguientes:



1. Organismo de Certificación (Certification Body)

Definición: Tercera parte independiente que realiza auditorías y otorga certificaciones de conformidad con los requisitos de las normas de sistemas de gestión (en este caso, ISO/IEC 27001).

💡 Aplicación: Específica que debe ser una entidad legalmente constituida e imparcial.

2. Cliente de Certificación / Organización Auditada.

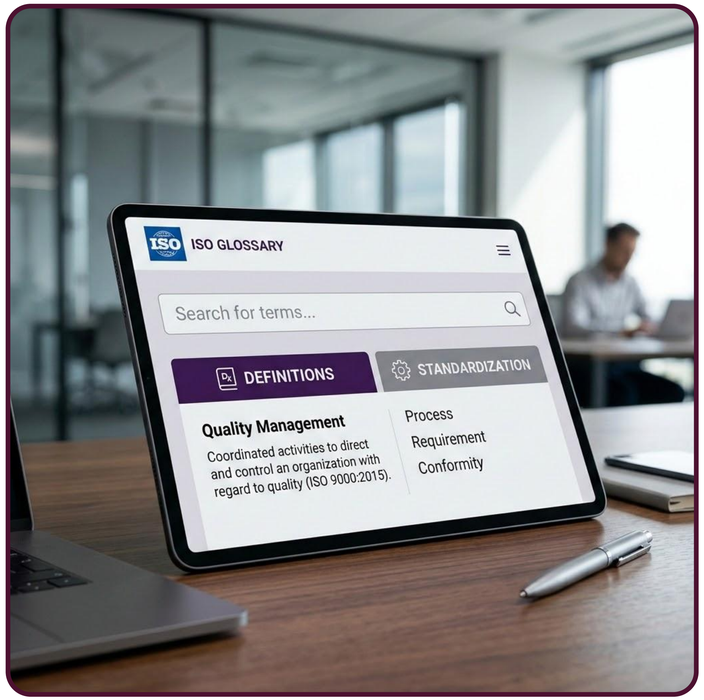
Definición: La entidad o empresa que solicita u obtiene la certificación de su SGSI.

💡 Aplicación: Delimita que el alcance del certificado solo cubre los activos, procesos y personal que están bajo el control directo de este "cliente", algo vital al calcular los tiempos de auditoría en la nube o servicios tercerizados.

3. Términos y definiciones

3. Personal bajo el Control de la Organización (Personnel under the organization's control)

Definición: Personas que realizan un trabajo para la organización o en su nombre, que puede impactar en el desempeño de la seguridad de la información.



💡 Aplicación: Este término se volvió crítico en la actualización reciente, ya que aclara que el cálculo de empleados para determinar los días de auditoría no solo incluye a los empleados en nómina directa (internal staff), sino también a contratistas independientes y personal externo que opere dentro del alcance del SGSI.

4. Competencia (Competence)

Definición: Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

💡 Aplicación: En el contexto de la norma, separa la "competencia" (saber auditar en la práctica) de la simple "calificación" (tener un diploma en papel).

3. Términos y definiciones

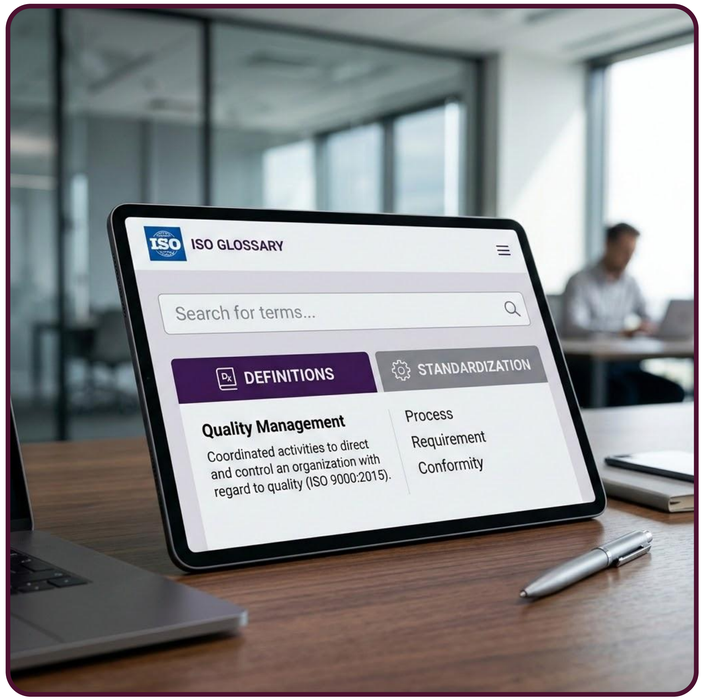
5. Auditoría Remota (Remote Audit)

Definición: Facilitación de la auditoría de un sitio o proceso mediante el uso de medios electrónicos (TIC) para recopilar evidencia cuando no es posible o necesario el acceso físico.

⚖️ **Regla de Precedencia**

La Cláusula 3 opera bajo una regla jerárquica implícita: si un término técnico relacionado con la seguridad de la información tiene una definición en el diccionario común, pero tiene otra diferente en **la ISO/IEC 27000** o en esta cláusula, la definición de la norma anula cualquier otra interpretación.

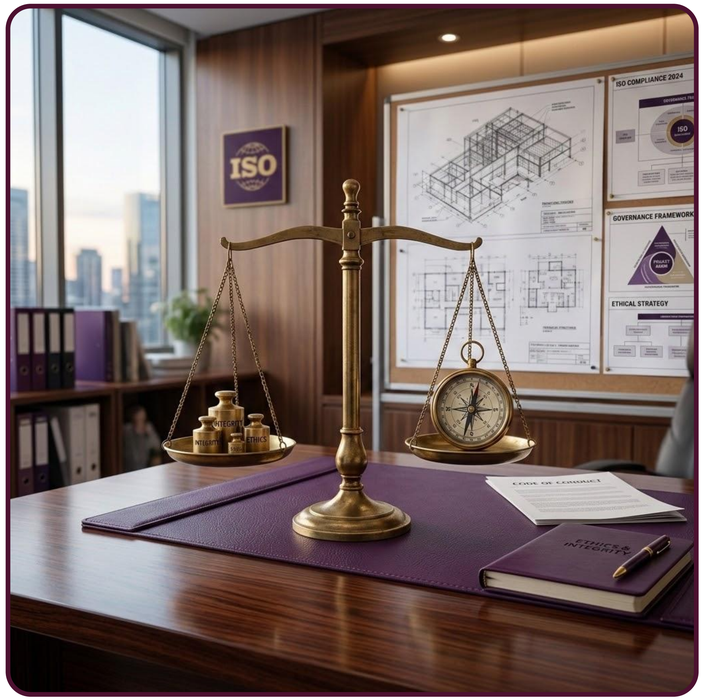
Esto garantiza que un juicio de auditoría se sostenga firmemente ante cualquier tribunal de apelación de certificación.



4. Principios generales

El marco de la norma se basa en principios y funciones clave que estructuran la evaluación:

Establece los pilares éticos y filosóficos sobre los cuales se sostiene todo el proceso de certificación de la seguridad de la información. Su cumplimiento garantiza que el mercado confíe en los certificados emitidos.



"Aplican los requerimientos de la ISO/IEC 17021-1:2015 4": La cláusula ***"(IS 4)"*** de la Norma 27006-1:2022 adopta los principios de la norma madre ISO/IEC 17021-1 en su cláusula 4, sin embargo se añade un enfoque estricto en ciberseguridad y protección de información.

Adopción por referencia directa y literal. Es una orden técnica que te dice: "No inventes nada nuevo para seguridad de la información; haz exactamente lo mismo que ya te exige la norma madre en ese punto específico".

El prefijo o sufijo "IS" (Information Security) se añade a aquellas cláusulas que contienen un requisito adicional, específico o modificado respecto a lo que ya establece la norma general de certificación (ISO/IEC 17021-1).

En la norma ISO/IEC 27006-1:2022, el anexo de mapeo es el Anexo B (Informativo), titulado oficialmente:

En español: Anexo B (Informativo) Correspondencia entre los requisitos de ISO/IEC 17021-1:2015 e ISO/IEC 27006-1:2022

4. Principios generales

📌 *Anexo B:*

- *1. Bloque de Imparcialidad (Cláusula 5)*

  -IS 4: Añade enfoque de Seguridad a los principios generales de auditoría.

  - 5.1: Idéntico. Contratos y personería jurídica estándar.

  -5.2 / IS 5.2.1: Modificación / Adición. Aplica la base de la 17021-1, pero la 27006-1 añade restricciones severas sobre consultoría en SGSI y herramientas de seguridad.

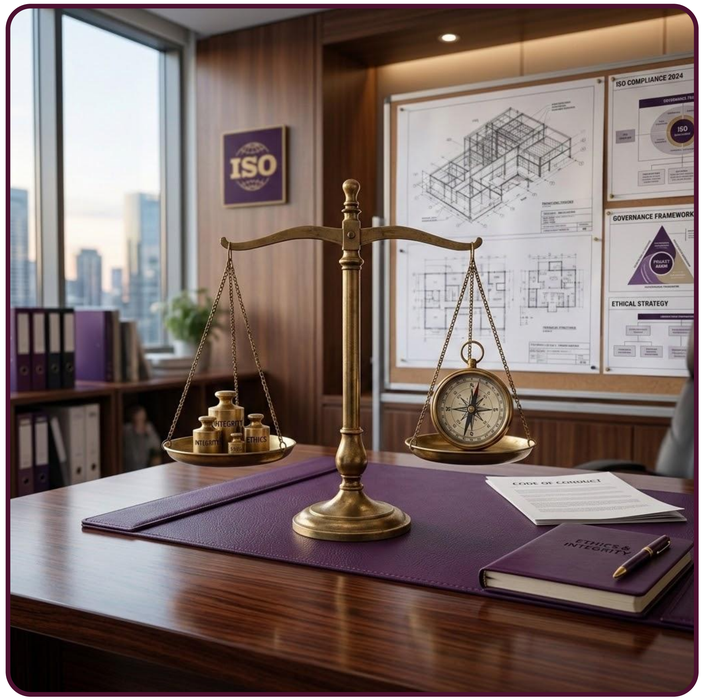
  -5.3 Idéntico. Seguros y estabilidad financiera general.

- *2. Bloque de Requisitos de Competencia (Cláusula 7)*

  -7.1 / IS 7.1.3: Adición de las tablas exactas de conocimientos que deben poseer los revisores del reporte y quienes toman la decisión final de otorgar el certificado ISO 27001.

  -7.2 / IS 7.2.2: Adición. Detalla cómo el organismo debe demostrar metodológicamente que sus auditores realmente conocen de ciberseguridad, legislación de datos, controles técnicos y gestión de riesgos antes de enviarlos a auditar.

  -7.3 / IS 7.3.1 / IS 7.3.2: Ampliación. Estructura los requisitos para los externos mediante acuerdos estrictos de confidencialidad y control de competencias específicas.



4. Principios generales

- ***3. Bloque del Proceso de Auditoría y Certificación (Cláusula 9)***

  Este es el bloque más denso y donde el prefijo IS aparece con más fuerza, porque el proceso para auditar un sistema de ciberseguridad varía mucho respecto a una auditoría común:

  -9.1 / IS 9.1.3 : Adición. Regula el cálculo de tiempos de auditoría y, críticamente en la versión 2024, introduce el marco para auditar organizaciones en la nube (virtuales).

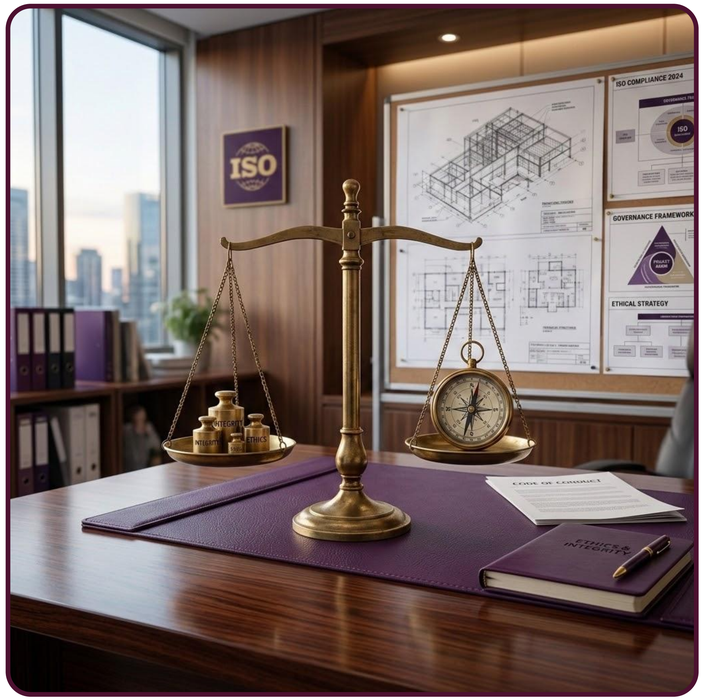
  -9.2 / IS 9.2 (Auditoría Inicial - Etapa 1): Modificación, Establece qué debe buscar obligatoriamente el auditor en la Etapa 1 (como el Análisis de Brechas, Declaración de Aplicabilidad - SoA, e identificación de activos) antes de dar luz verde para ir a revisar los controles en la Etapa 2.

  -9.3 / IS 9.3 (Auditoría Etapa 2): Adición. Exige recolectar evidencia específica de la efectividad de los controles del Anexo A de la ISO 27001.

  -9.4 / IS 9.4: Adición. Exige que el reporte final de auditoría documente expresamente el alcance del SGSI de forma clara, los controles del Anexo A de la ISO 27001 que fueron validados, y si se utilizaron técnicas de auditoría remota.

  -9.5: Idéntico. El proceso de toma de decisión sigue las reglas generales de la 17021-1.

  -9.6:Idéntico. Los ciclos de tres años y vigilancias anuales se mantienen sin cambios específicos.



4. Principios generales

Principios: Fundamentos para los requisitos de desempeño y operación que guían las decisiones:

- **Imparcialidad:** Necesaria para la confianza en la certificación.

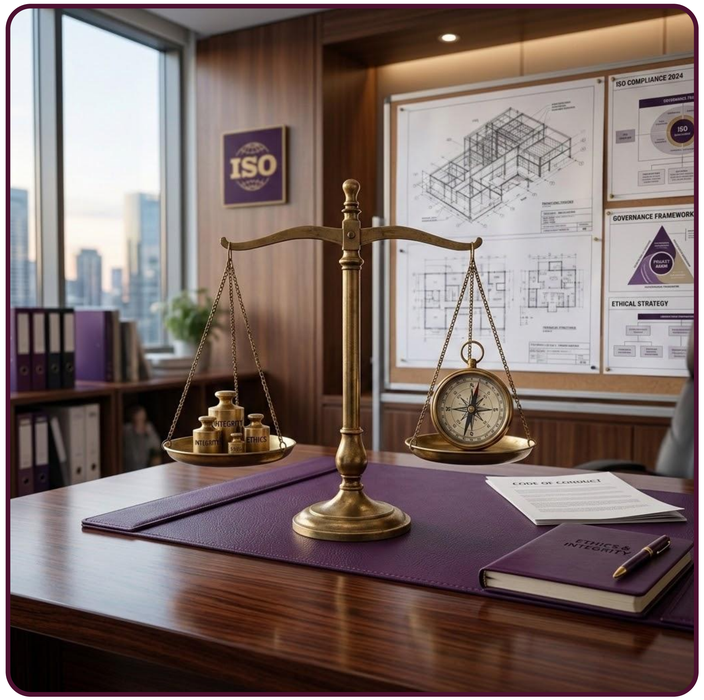
  Es el principio más crítico. El organismo de certificación debe ser y parecer totalmente neutral.

  💡 Enfoque en Seguridad: Significa que una misma empresa no puede hacer la consultoría para implementar la ISO 27001 y, al mismo tiempo, actuar como la casa certificadora que evalúa ese sistema. Esto sería un conflicto de intereses directo ("ser juez y parte").

- **Competencia:** La certificación de un SGSI solo es valiosa si quienes la ejecutan saben realmente lo que están haciendo.

  💡 Enfoque en Seguridad: Los auditores no solo deben saber "cómo auditar", sino que deben poseer un conocimiento técnico profundo en riesgos tecnológicos, vulnerabilidades, leyes de privacidad (como GDPR) y controles de seguridad (como criptografía o seguridad en la nube).

- **Responsabilidad:** La organización auditada es la única responsable de cumplir de forma continua con los requisitos de la ISO 27001. La casa certificadora es responsable de evaluar la evidencia objetiva de dicho cumplimiento y tomar una decisión basada en ella. El certificado no exime a la empresa de su responsabilidad ante un ciberataque.



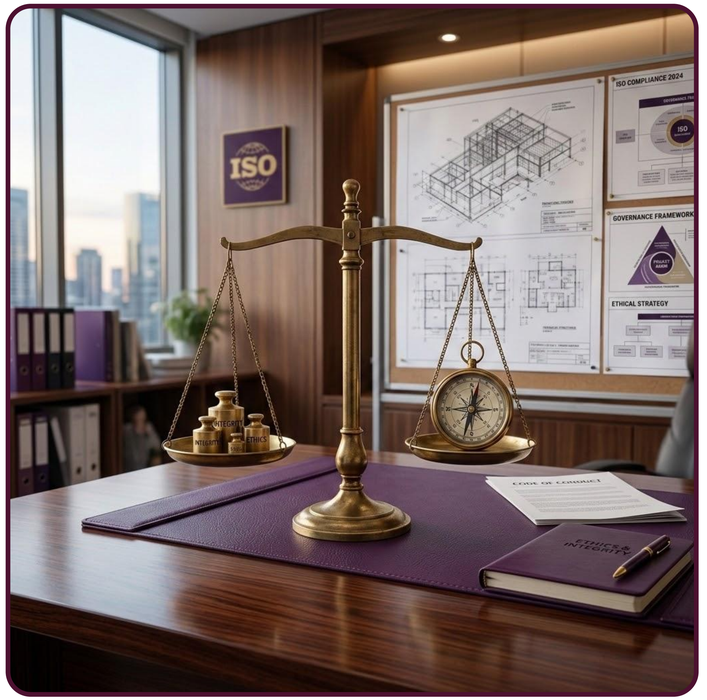
4. Principios generales

- **Transparencia:**El organismo de certificación debe poner a disposición del público (o proporcionar cuando se solicite) **información oportuna sobre sus procesos de auditoría**, esquemas de certificación y el estado de cualquier certificación otorgada.

- **Confidencialidad:** Para evaluar un SGSI, los auditores tienen acceso a las entrañas tecnológicas y estratégicas de una empresa.

  💡 Enfoque en Seguridad: Exige el resguardo absoluto de la información del cliente, implementando controles estrictos para que los datos recabados en la auditoría jamás se filtren o expongan.

- **Enfoque basado en riesgos:** Las casas certificadoras deben gestionar sus propios riesgos al operar. Esto implica evaluar el riesgo de emitir un certificado incorrecto a una empresa que no lo merece, lo cual dañaría la reputación de todo el ecosistema ISO a nivel mundial.



4. Principios generales

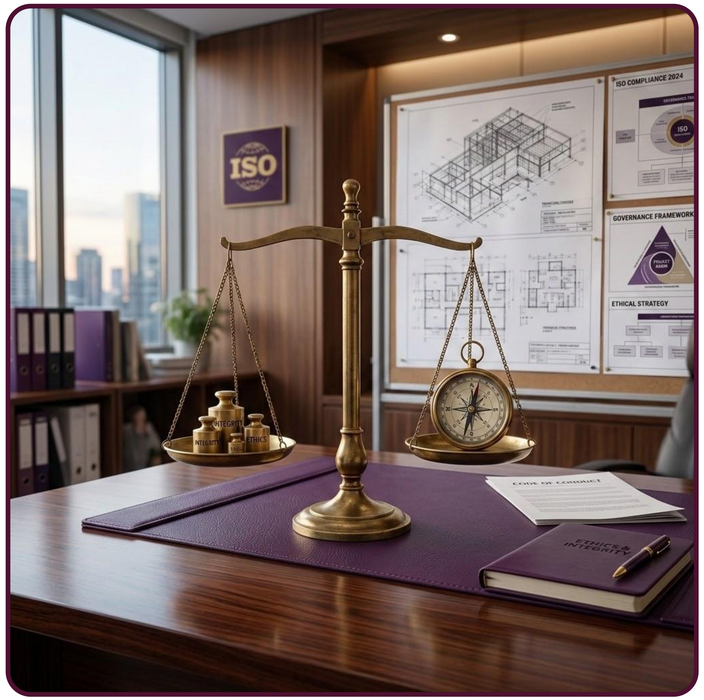
🛠️ ¿Cómo se aplican estos principios en el día a día?

Para que estos principios no se queden solo en buenas intenciones, la norma exige más adelante que se traduzcan en acciones concretas:

- Comités de Imparcialidad: Las certificadoras crean comités independientes formados por partes interesadas externas (asociaciones, clientes, académicos) para revisar que la empresa no esté favoreciendo a ciertos clientes.

- Evaluación y Registros de Competencia: Los auditores son evaluados periódicamente mediante exámenes técnicos y auditorías atestadas (un auditor senior evalúa a un auditor junior en el campo) para asegurar que mantienen su nivel técnico actualizado frente a las amenazas del 2026.

💡 De igual manera se debe tener un registro que demuestre competencias y experiencia sobre las auditorías.



5. Requisitos generales

Si la Cláusula 4 definía la filosofía y los principios éticos, la Cláusula 5 traduce esos principios en requisitos legales y contractuales obligatorios que un Organismo de Certificación debe cumplir para poder operar legítimamente.

Esta sección toma como base la estructura de la ISO/IEC 17021-1 y le añade candados específicos para el sector de la seguridad de la información.

5.1 Cuestiones legales y contractuales.

5.2 Gestión de la imparcialidad.

5.3 Responsabilidad legal y financiamiento.

🎯 El impacto real en la Seguridad de la Información

La Cláusula 5 existe para proteger la integridad del mercado. Si se permitiera que una empresa de ciberseguridad instalara los firewalls, redactara las políticas de una organización y luego esa misma empresa le otorgara el certificado ISO 27001, el certificado perdería toda su credibilidad.

5. Requisitos generales

5.1 Cuestiones legales y contractuales

Aplican los requerimientos de la ISO/IEC 17021-1:2015 5.1

💡 Recuerda, Adopción por referencia directa y literal. Es una orden técnica que te dice: "No inventes nada nuevo para seguridad de la información; haz exactamente lo mismo que ya te exige la norma madre en esta sub cláusula específica", dentro del anexo B se identifica como Idéntico.

5. Requisitos generales

5.2 Gestión de la imparcialidad

Esta cláusula establece los límites estrictos que un organismo de certificación (OC) debe respetar para garantizar que sus decisiones de certificación de un SGSI no estén sesgadas por intereses comerciales, relaciones de consultoría previa u otras actividades relacionadas con la seguridad de la información.

El organismo debe asegurar lo siguiente:

- **(IS 5.2.1) General: Aplican los requerimientos de la ISO/IEC 17021-1:2015 5.2. adiciona los requerimientos en 5.2.2.**

  💡 Recuerda, dentro del anexo B esta como Modificación / Adición. Aplica la base de la 17021-1, pero la 27006-1 añade restricciones severas sobre consultoría en SGSI y herramientas de seguridad.

- **5.2.2 Conflictos de Interés:** El organismo de certificación no debe proporcionar servicios de consultoría de sistemas de gestión de la seguridad de la información (SGSI).

  Restricción sobre auditorías internas del cliente: El organismo de certificación no debe realizar auditorías internas del SGSI del cliente de certificación.

  Mitigación y gestión de relaciones comerciales (Riesgos a la imparcialidad): El organismo de certificación debe identificar, analizar y documentar los riesgos relacionados con conflictos de intereses que surjan de la provisión de certificación, incluyendo cualquier conflicto que surja de sus relaciones. El hecho de que otra parte del organismo de certificación, o una entidad legal relacionada, proporcione consultoría de SGSI constituye una amenaza inaceptable a la imparcialidad.

5. Requisitos generales

5.2 Gestión de la imparcialidad

En resumen: La Cláusula 5.2 obliga al organismo de certificación a identificar y mitigar de forma continua cualquier conflicto de interés o presión comercial que amenace su neutralidad. Prohíbe estrictamente ofrecer servicios de consultoría o auditorías internas de SGSI a los mismos clientes de certificación. Además, impone un veto obligatorio de 24 meses a cualquier auditor que haya asesorado previamente a la organización auditada.

5. Requisitos generales

5.3 Responsabilidad legal y financiamiento

Aplican los requerimientos de la ISO/IEC 17021-1:2015 5.3

💡 Recuerda, Adopción por referencia directa y literal. Es una orden técnica que te dice: "No inventes nada nuevo para seguridad de la información; haz exactamente lo mismo que ya te exige la norma madre en esta sub cláusula específica", dentro del anexo B se identifica como Idéntico.

6. Requisitos estructurales

Aplican los requerimientos de la ISO/IEC 17021-1:2015 6.

💡 Ojo la cláusula 6 no está dentro del anexo B aún cuando está indicado que se aplican los requerimientos de la 17021-1, motivo:

El Capítulo 6 (Requisitos de Estructura) es un desierto absoluto de cambios. No tiene cambios en sus subcláusula. Es un bloque 100% plano de principio a fin; En la técnica de redacción de la ISO, cuando un capítulo entero es idéntico y no tiene ninguna ramificación con esteroides de ciberseguridad, se aplica el principio de omisión por bloque. El Anexo B prefiere borrar el capítulo completo de la tabla para enviar un mensaje contundente: "Aquí no hay nada que añadir, ni al principio, ni al medio, ni al final".

7. Requisitos del Proceso

Esta cláusula define las competencias, conocimientos y habilidades que debe poseer el personal del organismo de certificación (auditores, revisores y personal técnico) que interviene en la auditoría y certificación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

7.1 Competencia del personal

7.2 Personal involucrado en las actividades de certificación

7.3: Uso de auditores externos individuales y expertos técnicos externos

7.4 Registros personales.

7.5 Outsourcing

7. Requisitos para los recursos

7.1 Competencia del personal

La cláusula 7.1 establece la obligación de que los organismos de certificación definan y verifiquen los conocimientos y habilidades de su personal. Exige un entendimiento profundo tanto de la gestión de la seguridad de la información como de las técnicas de auditoría específicas. Su propósito es garantizar que quienes evalúen un SGSI cuenten con el rigor técnico necesario para emitir un juicio confiable.

- **7.1.1 Consideraciones Generales: Aplican los requerimientos de la ISO/IEC 17021-1:2015 7.1.1 adiciona los requerimientos de 7.1.2 y 7.1.3.**

💡 Ojo la cláusula 7.1.1 tampoco está dentro del anexo B aún cuando está indicado que se aplican los requerimientos de la 17021-1, motivo:

Cualquiera pensaría que al decir "In addition" (Adicionalmente), la 7.1.1 debería ganarse una fila propia con la etiqueta IS en el Anexo B de mapeo. Sin embargo, no aparece listada de forma independiente por una razón de técnica de indexación y limpieza de tablas.

En la redacción técnica de ISO, la cláusula 7.1.1 no contiene un requisito técnico de ciberseguridad por sí misma (Cláusula General). No te dice qué tienes que hacer; funciona simplemente como un "letrero de tránsito" o un enrutador que te avisa: "Ojo, aplica la norma general, pero si quieres ver las adiciones reales de seguridad de la información, camina hacia las cláusulas 7.1.2 y 7.1.3".

7. Requisitos para los recursos

7.1 Competencia del personal

- **(IS 7.1.2) Criterios de competencia para auditores de SGSI:** Los auditores que realicen auditorías de SGSI deben poseer conocimientos y habilidades **(referenciadas en la tabla A1 DE LA ISO 17021-1)** que abarquen lo siguiente:

a) Terminología, principios, gestión y técnicas de seguridad de la información.

b) Normas de sistemas de gestión de la seguridad de la información (por ejemplo, ISO/IEC 27001).

c) Principios y técnicas de gestión del riesgo de seguridad de la información.

d) Aplicación de controles de seguridad de la información de acuerdo con las mejores prácticas y regulaciones pertinentes.

e) Leyes, regulaciones y otros requisitos legales específicos del sector de la seguridad de la información que sean relevantes para el alcance de la auditoría.

f) Comprensión de los procesos de negocio y las tecnologías operativas del cliente evaluado.

Se adicionan los requerimientos de 7.1.3 y 7.2.2.

💡 Define con precisión milimétrica los conocimientos específicos que un auditor de la norma debe demostrar activamente en el campo. Cubre desde la terminología de seguridad, técnicas de mitigación de riesgos y leyes aplicables, hasta los controles técnicos. Busca que el auditor identifique fallas reales en la seguridad y no se limite a hacer un simple checklist.

7. Requisitos para los recursos

7.1 Competencia del personal

📌 **Anexo A norma 17021-1 , se divide en:**

- **A.1 Consideraciones generales:** Este anexo especifica los conocimientos y habilidades que el organismo de certificación debe definir para cada función de certificación señalada en la cláusula 7.1. El personal involucrado en las actividades de certificación de SGSI debe poseer un nivel de conocimiento general o detallado según se especifica en las tablas correspondientes.

- **A.2 Tabla de requisitos de competencia (Matriz de Conocimientos):** El organismo de certificación debe asegurarse de que el personal demuestre conocimientos y habilidades en las siguientes áreas específicas para SGSI:

  -**Terminología** de seguridad de la información: Conceptos básicos, definiciones y vocabulario técnico (por ejemplo, ISO/IEC 27000).

  -Modelos y **controles** de seguridad: Comprensión de los controles de seguridad de la información y su aplicabilidad en diferentes entornos de negocio.

  -Gestión de **riesgos**: Métodos para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información.

  -Entorno del negocio del cliente: Comprensión de las prácticas comerciales, tecnologías y tipos de organizaciones que se van a auditar.

7. Requisitos para los recursos

7.1 Competencia del personal

📌 **Anexo A2 norma 17021-1:** Es el núcleo operativo del anexo que desglosa en una tabla exacta los temas que el personal debe dominar por función. Divide los requisitos entre **auditores de campo, revisores de informes y tomadores de decisiones finales**. Exige niveles diferenciados de conocimiento (profundo o general) según el impacto de la tarea.

7. Requisitos para los recursos

7.1 Competencia del personal

- **(IS 7.1.3) Criterios de competencia para el personal que revisa los informes de auditoría y toma decisiones de certificación:** El personal que revisa los informes de auditoría y toma las decisiones sobre la certificación debe tener el conocimiento y la comprensión necesarios para verificar que los hallazgos de la auditoría y las conclusiones de los equipos de auditoría cumplen con los requisitos de la norma de certificación y el alcance solicitado. Este personal debe demostrar competencia en la evaluación del impacto de las no conformidades identificadas en la efectividad global del SGSI del cliente.

💡 La subcláusula 7.1.3 es sumamente estricta. El comité o la persona que firma la certificación final no puede ser un administrativo que solo cuenta firmas y hojas. Si no entienden el impacto de una vulnerabilidad reportada en el informe, no están listos para tomar la decisión. Capacitarlos igual o más que a un auditor en S.I. es fundamental.

7. Requisitos para los recursos

7.1 Competencia del personal

- **7.1.4: Evaluación de Competencia:** Establece el requisito de que los organismos de certificación evalúan formalmente a su personal antes de asignarle responsabilidades de auditoría o certificación, utilizando métodos efectivos y documentando todo el proceso. Esto asegura que solo las personas con el nivel de conocimiento adecuado **(como se define en la Cláusula 7.1.3 y el Anexo A)** realicen tareas técnicas críticas.

1. Requisito de Evaluación Formal: El organismo de certificación debe tener un proceso para evaluar y verificar formalmente la competencia de todo el personal involucrado en las actividades de auditoría y certificación antes de su asignación.

💡 No basta con decir que un auditor es bueno; tienes que demostrarlo antes de que toque un sistema real. Piensa en esto como una "prueba de manejo" para tus auditores de SGSI; si no pueden demostrar su competencia en un entorno controlado, no los dejes entrar a la "carretera" con un cliente.

7. Requisitos para los recursos

7.1 Competencia del personal

2. Definición de Métodos de Evaluación: El organismo de certificación debe definir los métodos de evaluación que se utilizarán para determinar si el personal posee el conocimiento necesario (véase 7.1.3 y el Anexo A).

💡 Tienes flexibilidad para elegir cómo evaluar (exámenes, simulaciones, revisiones de informes), pero el método debe ser efectivo. No hagas preguntas de opción múltiple fáciles; diseña escenarios que realmente prueben si entienden cómo un control de seguridad impacta en el riesgo del negocio.

3. Criterios de Evaluación y Aplicación: Los métodos de evaluación deben diseñarse para garantizar la consistencia en la aplicación de los criterios de competencia definidos y deben incluir medios para medir la efectividad de la evaluación.

💡 La competencia no es una opinión subjetiva. Asegúrate de que todos los evaluadores utilicen la misma "vara de medir" y de que tu proceso de evaluación sea auditable y justo. Si dos evaluadores califican de manera muy diferente la misma respuesta, tu proceso tiene un problema de consistencia.

7. Requisitos para los recursos

7.1 Competencia del personal

4. Registros de Evaluación de Competencia: Se deben mantener registros de la evaluación y la competencia demostrada por todo el personal de auditoría y certificación.

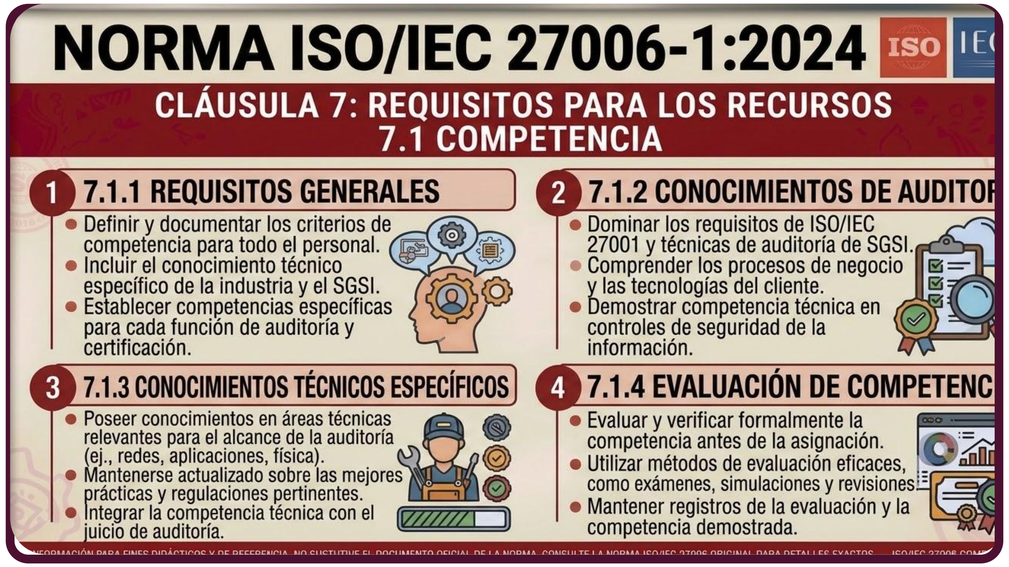
💡 "Si no está escrito, no sucedió". Tienes que poder mostrar las pruebas de que cada auditor y tomador de decisiones ha pasado sus evaluaciones técnicas. Este es tu "pasaporte de competencia" para el mercado.

7. Requisitos para los recursos

7.1 Competencia del personal

En resumen: Esta cláusula Obliga al organismo a mapear y documentar las competencias necesarias para cada rol del proceso de certificación. Remite directamente al Anexo A de la norma 17021-1, el cual contiene la tabla detallada de conocimientos requeridos. Asegura que ninguna persona sin la competencia demostrada participe en la evaluación o toma de decisiones del SGSI.

La certificación CHIEF AUDITOR otorga acceso a un registro de competencias para dar cumplimiento a esta subcláusula.



7. Requisitos para los recursos

7.2 Personal involucrado en las actividades de certificación

Esta sección establece los requisitos obligatorios e indispensables que los organismos de certificación deben asegurar y demostrar respecto a los conocimientos, la formación, la experiencia y los criterios de selección de los auditores y el personal que interviene en el proceso de certificación de un SGSI.

- **(IS 7.2.1) General: Aplican los requerimientos de la ISO/IEC 17021-1:2015 7.2 y se adicionan requerimientos en 7.2.2.**

- **7.2.2 Demostración de los conocimientos y la experiencia del auditor:** El organismo de certificación debe demostrar que cada auditor tiene conocimientos y experiencia a través de cada uno de los siguientes puntos:

  a) Cualificaciones reconocidas específicas de SGSI;

  b) Registro como auditor, cuando sea aplicable;

  c) Participación en cursos de formación en SGSI;

  d) Auditorías de SGSI presenciadas por otro auditor de SGSI; y

  e) Desarrollo profesional continuo de conocimientos y las habilidades.

💡 El organismo de certificación debe tener un expediente impecable donde se demuestre con papeles, cursos y auditorías supervisadas que el auditor realmente sabe en un entorno de SGSI.

7. Requisitos para los recursos

7.2 Personal involucrado en las actividades de certificación

- **7.2.2.2: Selección de auditores**

Los criterios para la selección de los auditores de SGSI deben garantizar que cada auditor:

a) Cuenta con educación profesional o formación equivalente al nivel universitario;

b) Ha completado con éxito al menos cinco días de formación, cuyo alcance cubra las auditorías de SGSI y la gestión de auditorías;

c) Tiene al menos cuatro años de experiencia laboral a tiempo completo en tecnología de la información, de los cuales al menos dos años deben estar en un rol o función relacionada con la seguridad de la información.

💡 Traducción práctica: se acabó el improvisar. La norma exige que para auditar un SGSI necesitas kilómetros recorridos. Esos cuatro años en TI y dos dedicados exclusivamente a la seguridad de la información actúan como un filtro "anti-teóricos". Asegúrate de que las hojas de vida de tus auditores reflejen funciones claras de seguridad (gestión de riesgos, firewalls, incidentes) y no solo soporte técnico general.

7. Requisitos para los recursos

7.2 Personal involucrado en las actividades de certificación

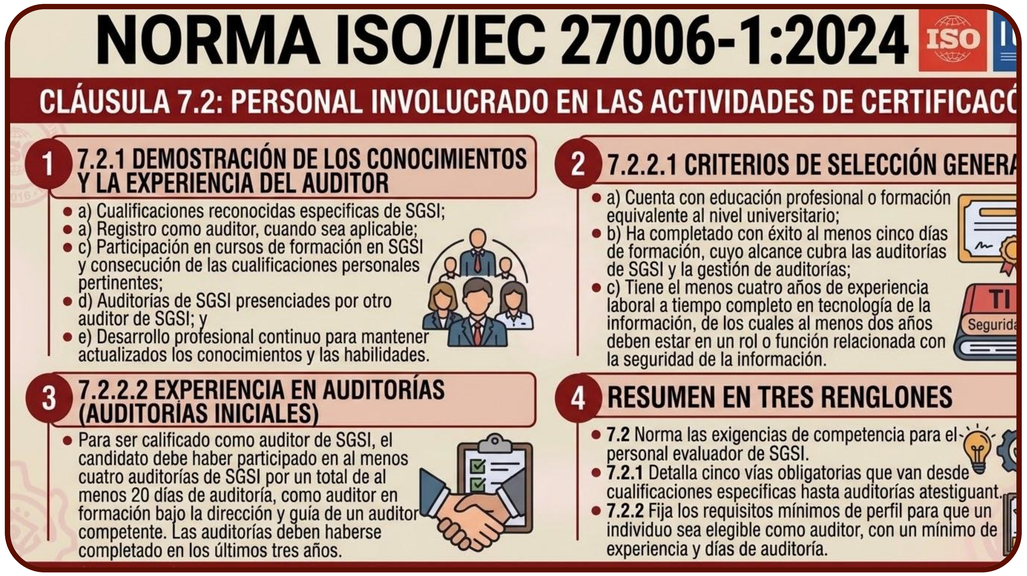
- **7.2.2.3 Experiencia en Auditorías (Auditorías Iniciales):** Para ser calificado como auditor de SGSI, el candidato debe **haber participado en al menos cuatro auditorías de SGSI para un total de al menos 20 días de auditoría, como auditor en formación bajo la dirección y guía de un auditor competente. Las auditorías deben haberse completado en los últimos tres años.**

💡 Es el equivalente en la auditoría a las "horas de vuelo" de un piloto. No puedes soltar a alguien a auditar un banco o una telco si antes no ha sudado la camiseta en al menos cuatro auditorías reales tutelado por un mentor. Consejo de amigo: documenta minuciosamente estas bitácoras de auditorías en formación, porque cuando la entidad de acreditación te revise, contará los días en el calendario uno por uno.

7. Requisitos para los recursos

7.2 Personal involucrado en las actividades de certificación

En resumen: Esta cláusula norma las exigencias de competencia para el personal evaluador de SGSI. Define la obligatoriedad de demostrar la experiencia y cualificaciones del equipo auditor. Restringe la asignación de auditorías únicamente a personal con habilidades técnicas validadas.:



7. Requisitos para los recursos

7.3: Uso de auditores externos individuales y expertos técnicos externos

Esta cláusula especifica las reglas y salvedades que debe considerar un organismo de certificación cuando decide contratar a personal externo (freelance, subcontratados o expertos técnicos en materias muy específicas de TI/seguridad) para completar su equipo de auditoría, asegurando que sigan bajo el control del organismo.

- **(IS 7.3.1) Aspectos generales:** Los requisitos de ISO/IEC 17021-1 se aplican. Adicionalmente, se aplican los siguientes requisitos específicos para SSGS en 7.3.2:

  El organismo de certificación debe asegurar que los auditores externos individuales y los expertos técnicos externos estén integrados en el equipo de auditoría de manera que se garantice que:

- a) operen de acuerdo con los procedimientos del organismo de certificación;
- b) sus competencias específicas en seguridad de la información, ciberseguridad y protección de la privacidad hayan sido verificadas para el alcance de la auditoría asignada;
- c) se definan claramente sus roles y responsabilidades dentro del equipo de auditoría; y
- d) sus actividades sean supervisadas y evaluadas por el organismo de certificación.

7. Requisitos para los recursos

7.3: Uso de auditores externos individuales y expertos técnicos externos

- **(IS 7.3.2) Requisitos específicos para el conocimiento y selección de externos:** El organismo de certificación debe asegurarse de que los auditores externos individuales y los expertos técnicos externos conozcan los procesos del organismo de certificación, incluidos sus requisitos de seguridad de la información y confidencialidad

💡 Antes de mandar a un "freelance" a auditar un SGSI, hazle una inducción documentada. No asumas que porque tiene 20 años de experiencia sabe cómo reportar las no conformidades tu organismo, ni cómo proteges tú los reportes de auditoría en la nube.

- **Cláusula 7.3.3: Requisitos adicionales para expertos técnicos:** Define los criterios específicos de competencia que deben cumplir los expertos técnicos que apoyan al equipo auditor en la evaluación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Su objetivo es garantizar que, si el auditor no posee el conocimiento tecnológico o sectorial hiper específico del cliente, el experto que lo acompañe sí lo tenga, asegurando la calidad de la auditoría.

  a) Conocimiento del SGSI y del contexto del cliente.

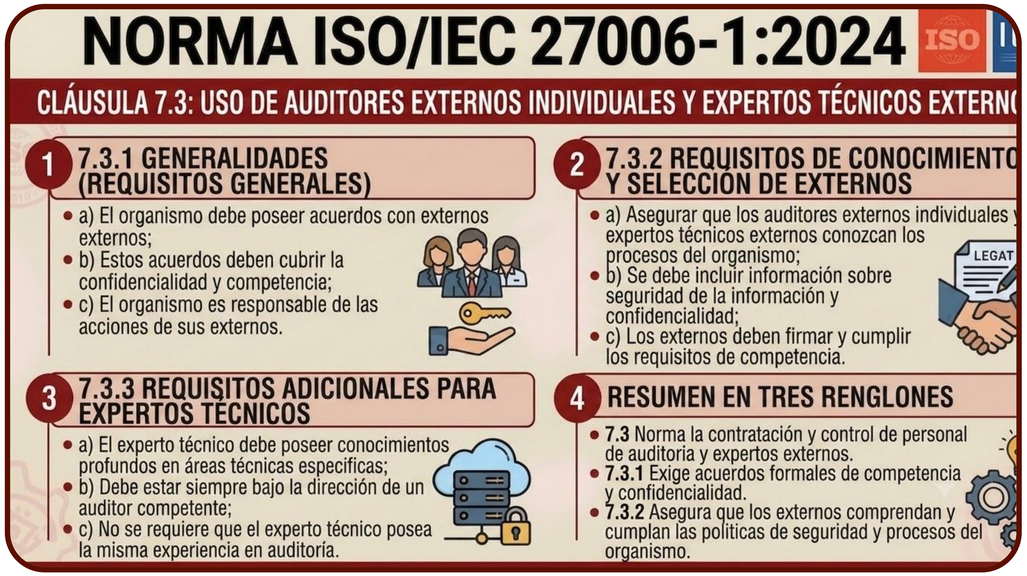
  b) El experto técnico debe tener conocimiento del área tecnológica o del sector industrial específico que se va a auditar.

  c) El experto técnico debe trabajar bajo la supervisión de un auditor.

7. Requisitos para los recursos

7.3: Uso de auditores externos individuales y expertos técnicos externos

En resumen: Esta cláusula regula la contratación y el uso de personal de auditoría y expertos técnicos ajenos a la plantilla fija del organismo. Exige que estos profesionales externos se rigen estrictamente por las mismas reglas de competencia y confidencialidad que el personal interno. Busca que el uso de terceros no diluya la calidad ni la seguridad del proceso de certificación.



7. Requisitos para los recursos

7.4 Registros del personal

Esta sección de la norma se ocupa del control, mantenimiento y actualización de los expedientes de todo el personal involucrado en los procesos de auditoría y certificación. Su propósito es garantizar que el organismo de certificación posea evidencia documental y verificable que demuestre de forma inequívoca que sus auditores, expertos técnicos y personal administrativo cumplen rigurosamente con las competencias, formación y experiencia exigidas para desempeñar sus funciones en el ámbito de la seguridad de la información.

- **7.4.1 Requisitos de los registros para el SGSI:** Los registros del personal del organismo de certificación deben incluir evidencia documentada que demuestre que cada miembro del personal (incluidos los auditores y expertos técnicos) cumple con los criterios de competencia específicos para el sector de la seguridad de la información establecidos en esta norma. Esto incluye el historial detallado de las auditorías de SGSI en las que han participado, los cursos de actualización profesional tomados en materia de seguridad informática, las cualificaciones específicas del sector y las evaluaciones periódicas de desempeño.

💡 La trampa del "Auditor Multiusos": Es muy común que los organismos de certificación quieran usar al mismo auditor estrella de calidad (ISO 9001) para el SGSI (ISO 27001). Cuidado. La cláusula 7.4 exige que la evidencia documental demuestre competencias específicas en seguridad de la información. Si en su expediente solo hay diplomas de gestión de procesos industriales, esa auditoría carece de validez normativa.

7. Requisitos para los recursos

7.4 Registros del personal

💡 **Recuerda: l**a ISO 27006-1:2022 es complementaria desde el punto de vista de seguridad de la información a la 17021-1 por lo que "**los requisitos de ISO/IEC 17021-1, 7.4 aplican",** por lo que no olvides que tu checklist debe validar que el organismo de certificación guarde los registros de PERFIL, FORMACIÓN, COMPETENCIA, EXPERIENCIA EN CAMPO, AFILIACIONES PROFESIONALES y su estatus.; El motivo de que la cláusula 7.4 no aparezca de forma explícita en la tabla del Anexo B se debe a una regla muy estricta de jerarquía y alcance en la arquitectura de las normas ISO; Se concluye que no se necesitan carpetas de expedientes especiales ni un archivero diferente para ciberseguridad. El método tradicional de guardar los currículums, las firmas de confidencialidad y los diplomas de tus auditores funciona exactamente igual y al no generar un cambio en la estructura de los expedientes, el Anexo B (que es una guía de excepciones de ciberseguridad) lo deja fuera para mantener la tabla compacta.

ISO/IEC 17021-1 CLÁUSULA 7.4:
CHECKLIST DE CUMPLIMIENTO (REGISTROS DEL PERSONAL)

CUMPLIMIENTO

Tipo de Registro	¿Qué debe incluir?
Perfil Profesional	Currículum vitae (CV) firmado, títulos y constancias laborales previas.
Evidencia de Formación	Certificados de cursos aprobados en la norma correspondiente (ej. Curso de Auditor Líder).
Evaluación de Competencia	Registros de los exámenes internos o listas de verificación de aptitud aplicadas por el OC.
Monitoreo en Campo	Formatos de evaluación de desempeño firmados por el evaluador que realizó la auditoría testigo.
Matriz de Autorización	Documento oficial vigente que indica sus competencias por código de sector industrial.

7. Requisitos para los recursos

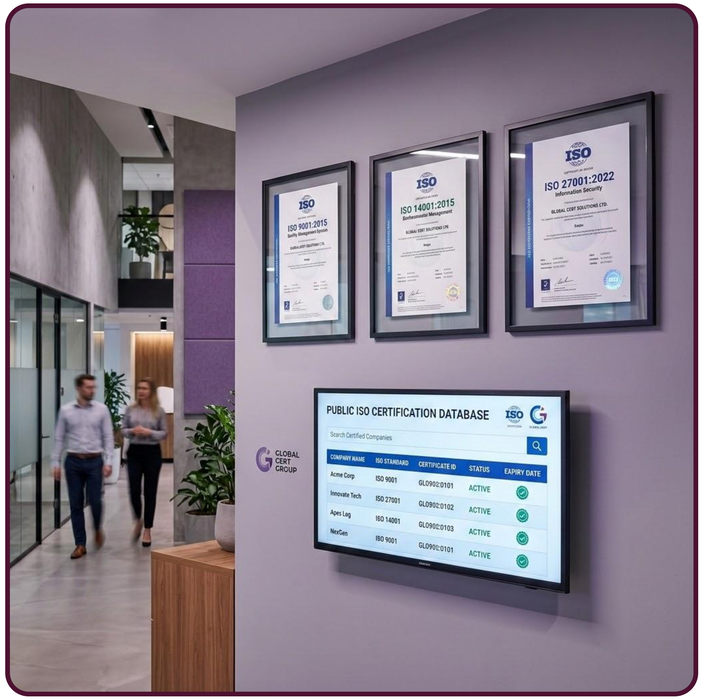
7.5 Subcontratación

Se aplican los requisitos de la norma ISO/IEC 17021-1, Cláusula 7.5.

💡 La cláusula 7.5 de la norma ISO/IEC 27006-1:2022 no desarrolla un texto operativo ni subcláusulas propias. En su lugar, adopta de manera íntegra, literal y por referencia directa las exigencias de la ISO/IEC 17021-1. Esto significa que la gestión de la subcontratación en SGSI no posee variaciones específicas en este estándar, No aparece en el Anexo B porque es 100% idéntica y plana por lo que se aplica la regla de la "Excepción de Bloque" (Igual que el Capítulo 6), como la cláusula 7.5 no se subdivide en la 27006-1 el Anexo B aplica su regla de oro: limpiar la tabla de todo lo que sea ruido innecesario. Si un proceso se ejecuta exactamente igual en una auditoría de Calidad (9001) que en una de Seguridad (27001), se borra del mapa de correspondencia para que el auditor concentre toda su energía mental en los puntos críticos de auditoría.

8. Requisitos de información

Esta sección establece los requisitos específicos de información que un organismo de certificación (OC) debe cumplir para garantizar la transparencia, la correcta emisión de los documentos de certificación y el uso adecuado de las marcas asociadas a la conformidad con ISO/IEC 27001. Su propósito es asegurar que tanto el público como las organizaciones certificadas cuenten con datos claros, verídicos y homologados sobre el alcance del SGSI.



8.1 Información pública.

8.2 Documentos de certificación.

8.3 Referencia a la certificación y uso de marcas.

8.4 Confidencialidad.

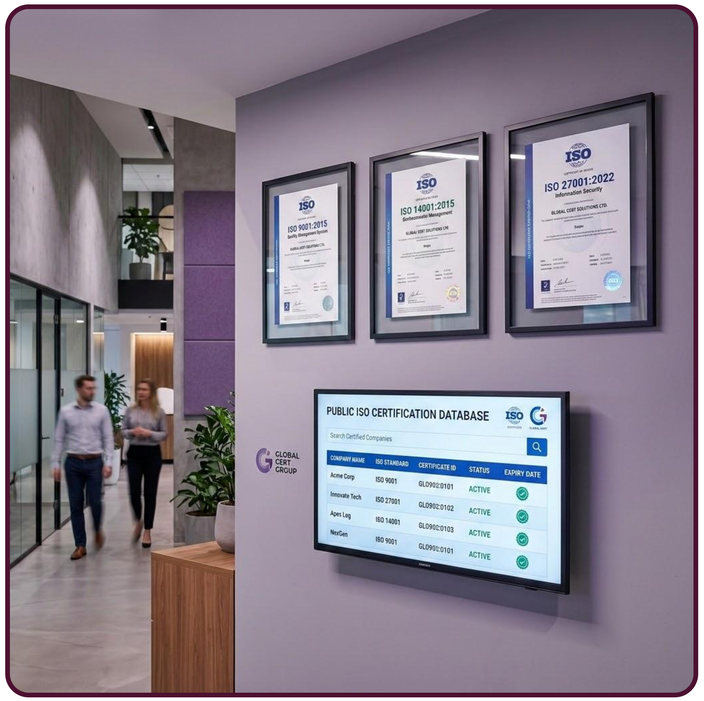
8.5 Intercambio de información.

8. Requisitos de información

8.1 Información pública

Se aplican los requisitos de la norma ISO/IEC 17021-1, Cláusula 8.1

💡 La cláusula 8.1 de la norma ISO/IEC 27006-1:2022 no desarrolla un texto operativo ni subcláusulas propias. En su lugar, adopta de manera íntegra, literal y por referencia directa las exigencias de la ISO/IEC 17021-1. Esto significa que la gestión de la subcontratación en SGSI no posee variaciones específicas en este estándar y por tal motivo no aparece en el anexo B.



8. Requisitos de información

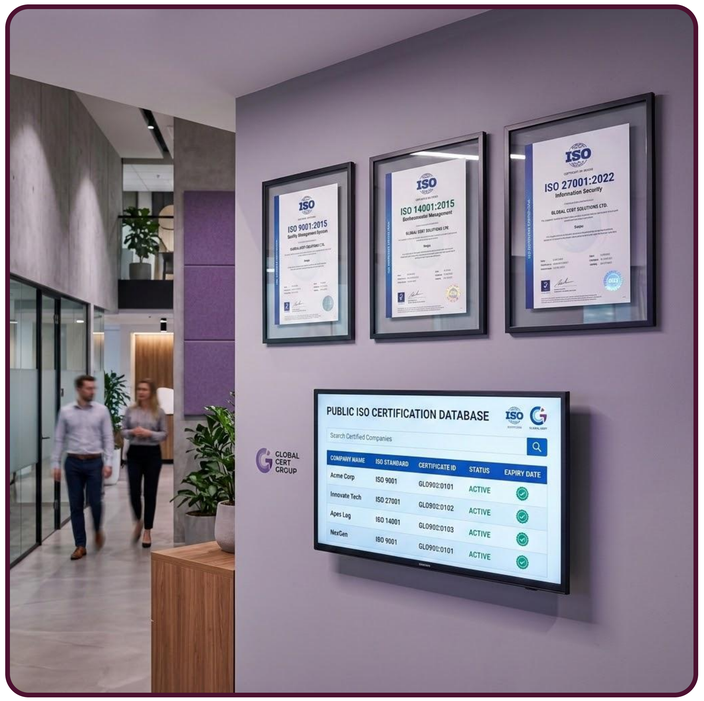
8.2 Documentos de certificación:

Se aplican los requisitos de la norma ISO/IEC 17021-1, Cláusula 8.2

💡 La cláusula 8.2 de la norma ISO/IEC 27006-1:2022 no desarrolla un texto operativo ni subcláusulas propias. En su lugar, adopta de manera íntegra, literal y por referencia directa las exigencias de la ISO/IEC 17021-1. Esto significa que la gestión de la subcontratación en SGSI no posee variaciones específicas en este estándar y por tal motivo no aparece en el anexo B.

(IS 8.2.1) Documentos de certificación - Generalidades: Se aplican los requisitos de la norma ISO/IEC 17021-1, Cláusula 8.2 en adición a los requerimientos de la cláusulas 8.2.2 y 8.2.3

⚠️ Nota de precisión sobre la 8.2: La razón por la que IS 8.2.1 (o la sección 8.2 en general) no aparece listada de esa forma en el Anexo B se debe a la reestructuración y limpieza de redundancias de la norma en su versión ISO/IEC 27006-1:2022; Al eliminarse las repeticiones del texto base de la 17021-1, las adiciones específicas para el diseño del certificado físico/digital quedaron redactadas directamente en el cuerpo del estándar (en la cláusula 8.2.2 de la nueva estructura), en lugar de depender de un anexo de mapeo para justificarse.



8. Requisitos de información

8.2 Documentos de certificación:

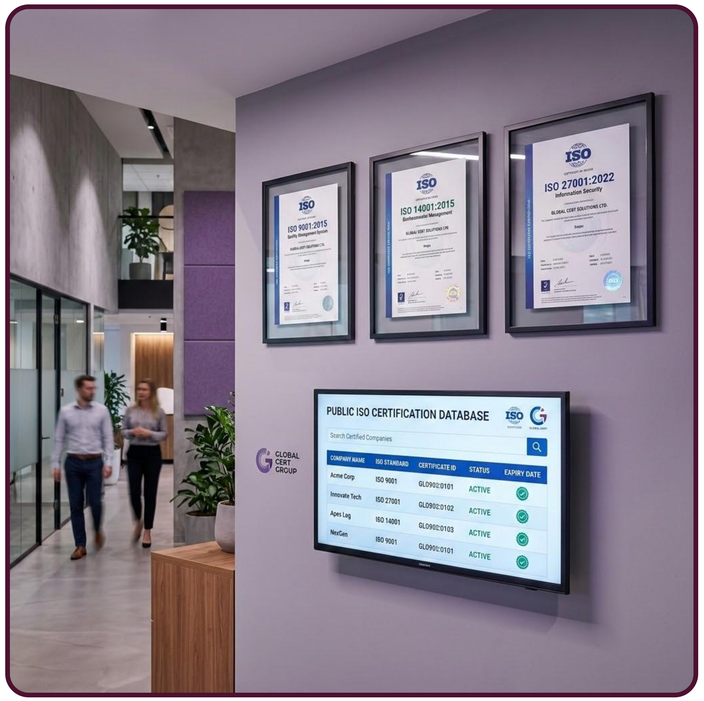
- **8.2.2: Requisitos para el Documento de Certificación (El Certificado):** Esta subcláusula establece los elementos exclusivos de ciberseguridad que el organismo de certificación debe incluir obligatoriamente dentro del texto del certificado impreso o digital:

  -Identificación de la Declaración de Aplicabilidad (SoA - Statement of Applicability): El certificado debe citar explícitamente la fecha y la versión exacta de la declaración de aplicabilidad que la organización audita y debe ligarse de manera explícita el nombre del documento SoA del cliente.

  -Claridad en la exclusión de controles: Si la organización excluyó controles permitidos del Anexo A de la ISO 27001, la mención al SoA en el certificado respalda legalmente qué controles aplican y cuáles no.

  -Nombre de la norma de controles aplicable: Debe indicar claramente que cumple con los requisitos de la norma ISO/IEC 27001:2022 (o la versión vigente en el momento).

  -**El Alcance Técnico Detallado:** Especificando claramente las sedes, plataformas, infraestructura tecnológica o procesos de negocio que quedan bajo el perímetro del SGSI.



- **Cláusula 8.2.3 Requisitos para la Definición del Alcance (Scope):** Esta subcláusula regula cómo se debe redactar y verificar el alcance de la certificación. En seguridad de la información, el "perímetro" de lo que está protegido debe ser clarísimo para evitar que una empresa certifique una pequeña oficina con 5 computadoras pero haga publicidad engañosa haciendo creer al mercado que toda su infraestructura global en la nube está certificada.

8. Requisitos de información

8.2 Documentos de certificación:

Los requerimientos IS adicionales obligan a cumplir con lo siguiente:

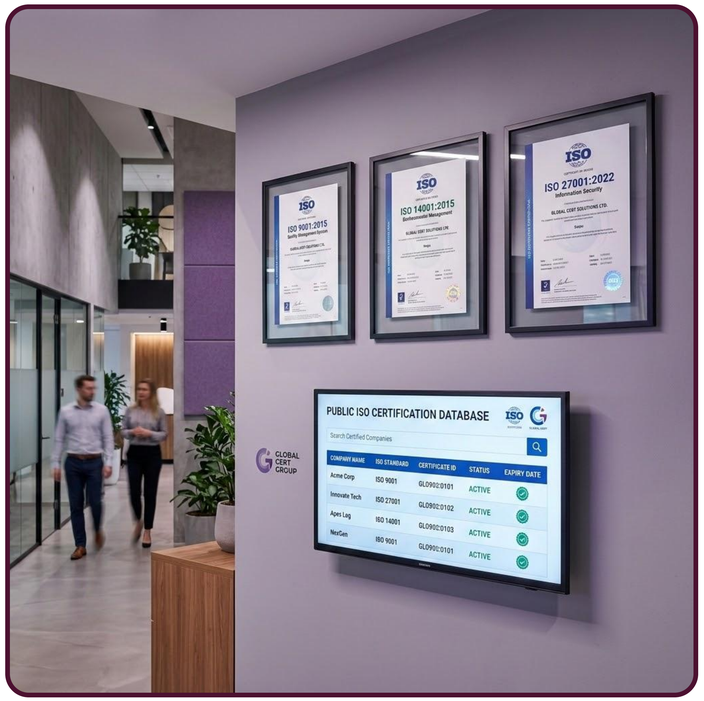
-Límites del SGSI perfectamente definidos: El alcance debe especificar con precisión los límites de la organización que han sido evaluados. Esto incluye detallar:

1. Las unidades de negocio o departamentos específicos (ej. "El departamento de desarrollo y soporte de la plataforma SaaS").

2. Las ubicaciones físicas (direcciones exactas de los centros de datos u oficinas involucradas) y los entornos virtuales o infraestructuras en la nube (ej. "asociado a la infraestructura Cloud en AWS región Virginia").

-Prohibición de alcances engañosos o parciales sin control: El organismo de certificación tiene prohibido aceptar o redactar un alcance que excluya procesos, servicios o herramientas que sean críticos para la seguridad de la actividad principal que se pretende certificar. Si un proceso afecta directamente la seguridad de la información del alcance, tiene que ser auditado.

-Interfaces y dependencias: El alcance plasmado debe dejar claro los puntos de contacto o interfaces con el exterior (por ejemplo, si el servicio certificado depende críticamente de un proveedor externo de hosting, la redacción del alcance debe ser transparente respecto a dónde termina la responsabilidad del cliente).

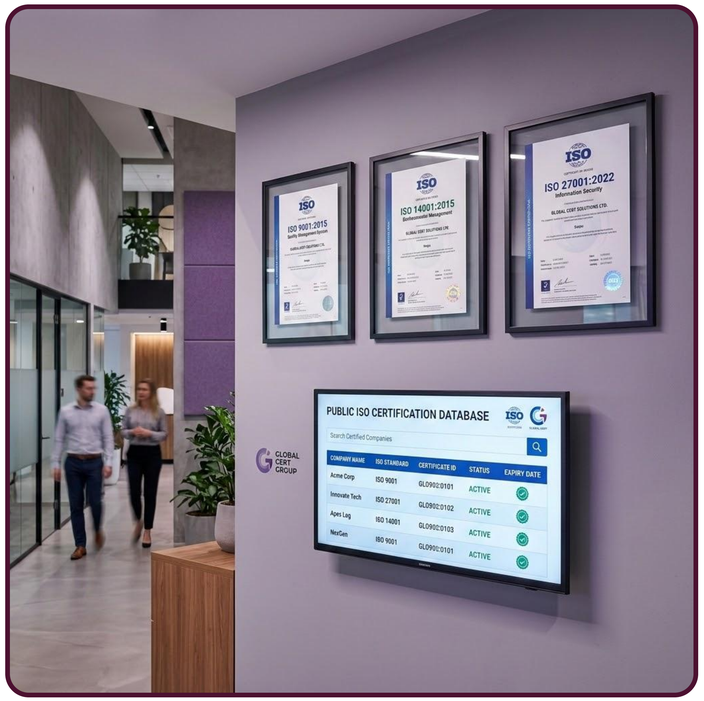


8. Requisitos de información

8.3 Referencia a la certificación y uso de marcas

Se aplican los requisitos de la norma ISO/IEC 17021-1, Cláusula 8.3

💡 La cláusula 8.3 de la norma ISO/IEC 27006-1:2022 no desarrolla un texto operativo ni subcláusulas propias. En su lugar, adopta de manera íntegra, literal y por referencia directa las exigencias de la ISO/IEC 17021-1. Esto significa que la gestión de la subcontratación en SGSI no posee variaciones específicas en este estándar y por tal motivo no aparece en el anexo B.Se debe garantizar que la marca de certificación no sea ambigua ni induzca a error.

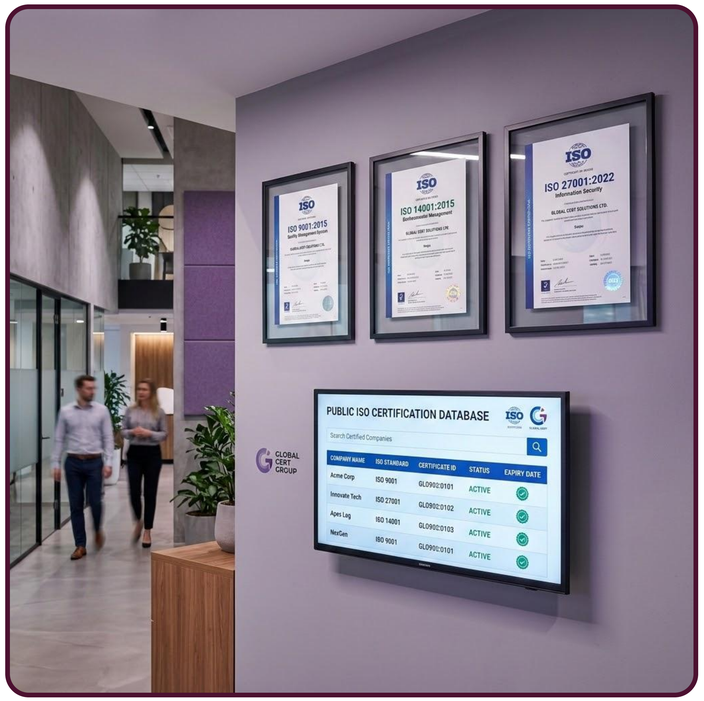


8. Requisitos de información

8.4 Confidencialidad

Se aplican los requisitos de la norma ISO/IEC 17021-1, Cláusula 8.4

💡 La cláusula 8.4 de la norma ISO/IEC 27006-1:2022 no desarrolla un texto operativo ni subcláusulas propias. En su lugar, adopta de manera íntegra, literal y por referencia directa las exigencias de la ISO/IEC 17021-1. Esto significa que la gestión de la subcontratación en SGSI no posee variaciones específicas en este estándar y por tal motivo no aparece en el anexo B.

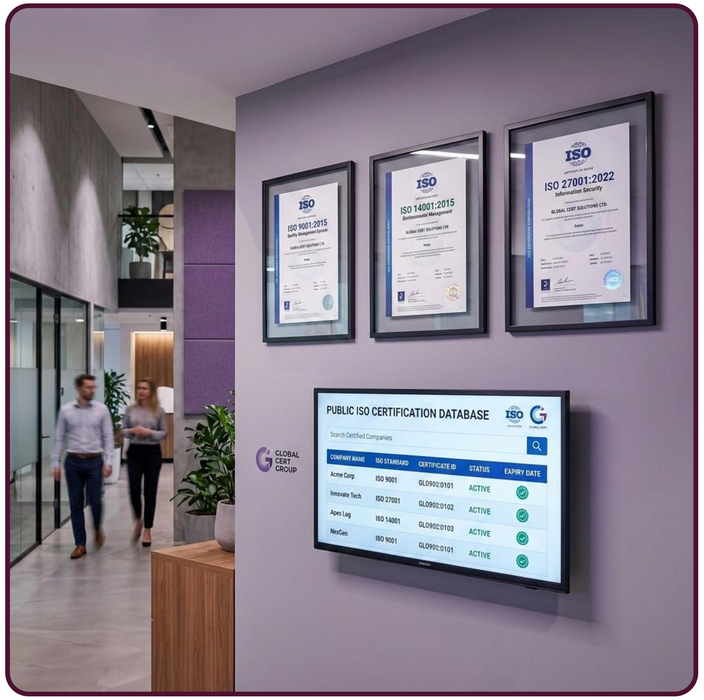


8. Requisitos de información

8.5 Intercambio de información

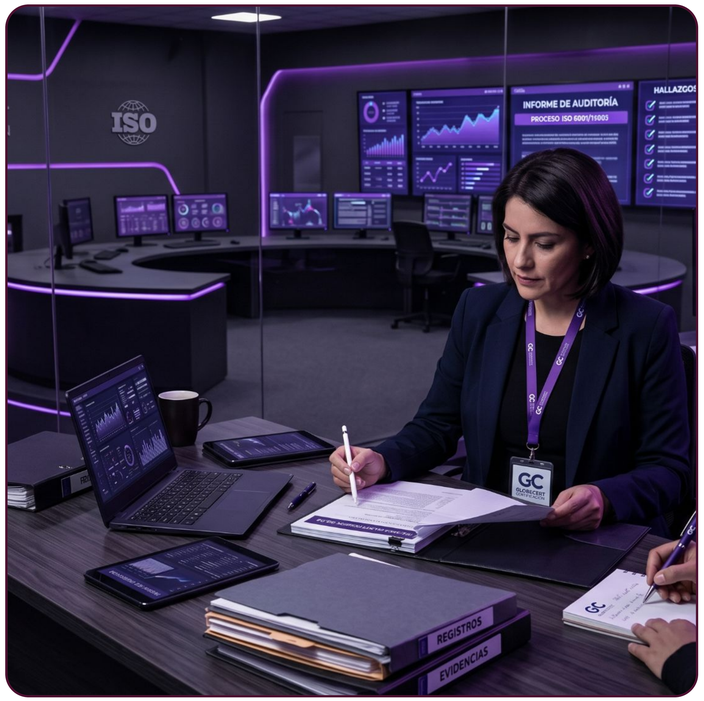
Se aplican los requisitos de la norma ISO/IEC 17021-1, Cláusula 8.5

💡 La cláusula 8.5 de la norma ISO/IEC 27006-1:2022 no desarrolla un texto operativo ni subcláusulas propias. En su lugar, adopta de manera íntegra, literal y por referencia directa las exigencias de la ISO/IEC 17021-1. Esto significa que la gestión de la subcontratación en SGSI no posee variaciones específicas en este estándar y por tal motivo no aparece en el anexo B.



9. Requisitos relativos a los procesos

La Cláusula 9 de la ISO/IEC 27006-1:2022 detalla las adaptaciones obligatorias y las reglas específicas que un organismo de certificación debe aplicar a lo largo de todo el ciclo de auditoría del SGSI. En lugar de inventar un proceso desde cero, esta cláusula actúa como un "filtro de seguridad de la información", determinando exactamente cómo calcular los tiempos de auditoría, cómo muestrear múltiples sitios, cómo auditar la Declaración de Aplicabilidad (SoA) y qué elementos técnicos específicos e indispensables deben verificarse en las Etapas 1 y 2.



9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

9.2 Planificación de las auditorías

Establece los preparativos específicos previos a la ejecución de la auditoría en campo.

9.3 Certificación inicial

Define las fases obligatorias para organizaciones que buscan certificarse por primera vez.

9.4 Realización de las auditorías

Describe las reglas metodológicas y de conducta que el equipo auditor debe seguir durante cualquier auditoría del ciclo.

9. Requisitos relativos a los procesos

9.5 Decisión de certificación
El núcleo que garantiza la imparcialidad del proceso.

9.6 Mantenimiento de la certificación
Regula el seguimiento obligatorio post-certificación.

9.7 Apelaciones
Establece el proceso para que los clientes soliciten la reconsideración de una decisión adversa tomada por el organismo de certificación.

9.8 Quejas
Regula la recepción, validación e investigación de expresiones de insatisfacción sobre las actividades del organismo o sus certificados.

9.9 Registros relativos a solicitantes y clientes
Define los requisitos para mantener registros de auditorías y certificaciones, asegurando confidencialidad y trazabilidad.

9. Requisitos relativos a los procesos

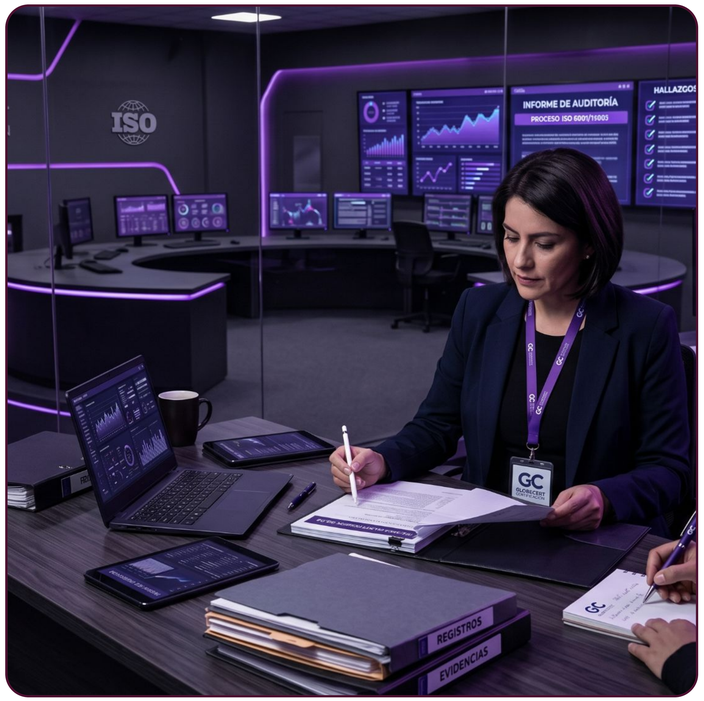
9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

Esta cláusula regula los pasos iniciales obligatorios que un organismo de certificación debe realizar antes de poner un pie en las instalaciones del cliente (o conectarse digitalmente). Su propósito es recopilar toda la información crítica del negocio del cliente, evaluar minuciosamente la complejidad de su entorno tecnológico, mapear los tipos de activos y determinar con bases técnicas (y mediante un análisis de riesgos formal) si es viable y seguro ejecutar auditorías remotas.

A nivel de estructura formal en el texto de la norma, esta sección se desglosa en seis sub cláusulas principales (de la 9.1.1 a la 9.1.6):

- **9.1.1 (Actividades previas a la certificación - Generalidades):** Aplican los requerimientos de ISO/IEC 17021-1:2015, 9.1.



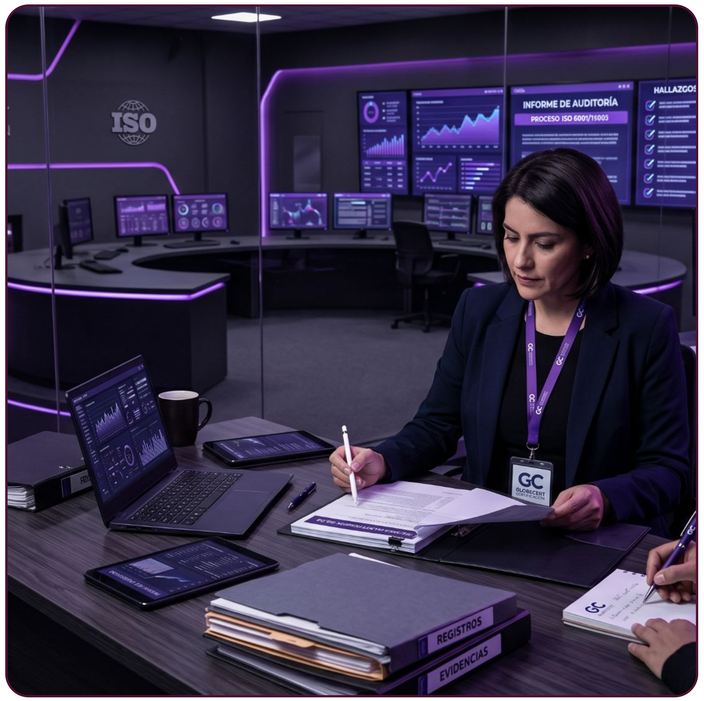
9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

- **9.1.2 Revisión de la solicitud (Application review):** El organismo de certificación debe revisar la solicitud y la información complementaria para asegurarse de que cuenta con la competencia necesaria para llevar a cabo la auditoría, determinar el tiempo de auditoría inicial requerido y confirmar que el alcance de la certificación propuesto es claro y técnicamente viable en relación con las operaciones de la organización.

- **(IS 9.1.3) Programa de auditoría (Audit programme):** Cuando se planee la utilización de técnicas de auditoría remota, el organismo de certificación debe realizar un análisis de riesgos detallado para determinar la viabilidad de su despliegue. Este análisis debe documentar la capacidad tecnológica del cliente, la estabilidad de los canales de comunicación, el acceso seguro a las evidencias electrónicas y el impacto potencial en la confidencialidad de la información auditada.



9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

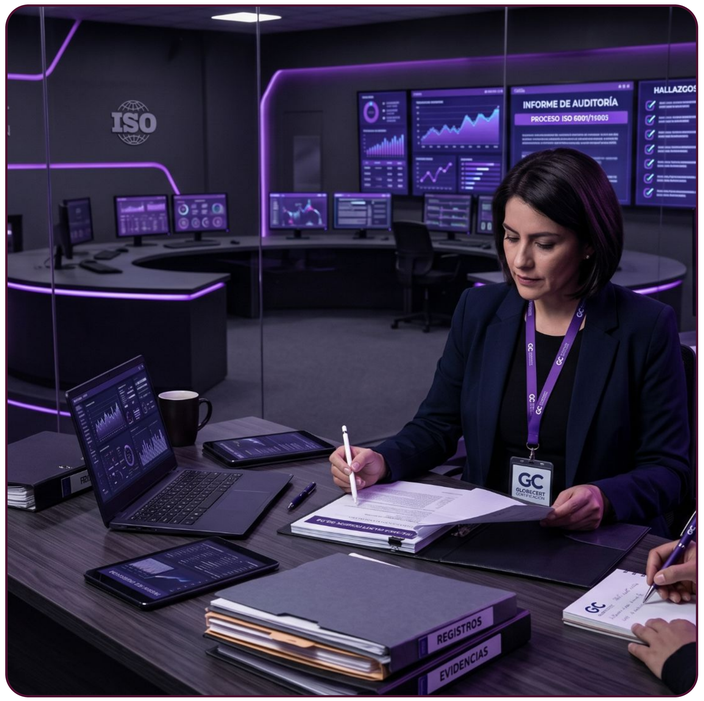
Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

- **9.1.4. Determinar tiempo de auditoría:** Esta sección establece las reglas obligatorias que un Organismo de Certificación (OC) debe seguir para calcular de manera realista y justificada el tiempo necesario para planificar y ejecutar una auditoría de un Sistema de Gestión de la Seguridad de la Información (SGSI).

  (IS 9.1.4.1): Generalidades: **Se aplican los requisitos de la norma ISO/IEC 17021-1:2015, 9.1.4. Adicionalmente, se deben aplicar los requisitos y la orientación dados en 9.1.4.2.**

  9.1.4.2: Tiempo de auditoría: El organismo de certificación debe utilizar el Anexo C para determinar el tiempo de auditoría

  NOTA Se proporciona orientación adicional y ejemplos sobre el cálculo del tiempo de auditoría en el Anexo D."



9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

📌 Anexo C para determinar el tiempo de auditoría:

Este anexo establece las tablas, factores de complejidad y fórmulas obligatorias para calcular el tiempo de auditoría. El cálculo se basa principalmente en e**l número de empleados que realizan trabajo bajo el control de la organización (dentro del alcance del SGSI) y se ajusta según factores de riesgo y complejidad tecnológica;** El organismo de certificación debe utilizar **el número efectivo de personal** como punto de partida para determinar el tiempo de auditoría. El tiempo mínimo de auditoría para un solo sitio se derivará de la Tabla C.1

TABLA C.1: TIEMPO MÍNIMO DE AUDITORÍA PARA UN SOLO SITIO (EXTRACTO NORMATIVO ESTÁNDAR)

NÚMERO EFECTIVO DE PERSONAL	TIEMPO MÍNIMO DE AUDITORÍA (DÍAS/AUDITOR)	STAGE 1 (REVISIÓN DOCUMENTAL)	STAGE 2 (AUDITORÍA IN-SITU/REMOTA)
1 a 10	2.5	0.5	2.0
11 a 15	3.0	1.0	2.0
16 a 25	3.5	1.0	2.5
26 a 45	4.5	1.0	3.5
46 a 65	5.5	1.5	4.0
66 a 85	6.0	1.5	4.5
86 a 125	7.0	2.0	5.0

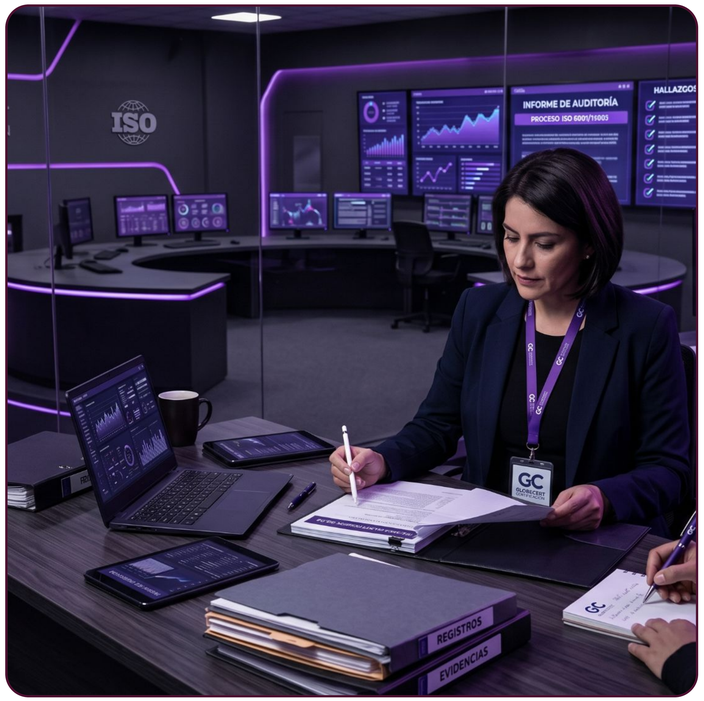
(Nota: La tabla continúa de forma proporcional para organizaciones más grandes, por ejemplo, más de 10,000 empleados requieren más de 30 días de auditoría base).

9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

C.2 Factores para ajustar el tiempo de auditoría (Complejidad y Riesgo): "El organismo de certificación debe considerar la complejidad del SGSI, el entorno de riesgo y el alcance de la subcontratación para ajustar el tiempo de auditoría base. Los ajustes deben ser documentados y justificados.").



Factores de Incremento (+) o Reducción (-) normados:

-Complejidad del negocio y criticidad de los datos: Procesamiento de datos sensibles (salud, financiero, militar).

-Entorno TI: Multiplicidad de plataformas tecnológicas, desarrollo de software propio o uso masivo de servicios Cloud.

-Madurez del sistema: Auditorías previas exitosas o un historial limpio de incidentes (permite reducciones leves).

-Sitios repetitivos: Si la organización opera en múltiples sitios idénticos (sucursales bancarias, almacenes), el tiempo total se puede optimizar bajo la regla de muestreo.

9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

📌Anexo D para determinar el tiempo de auditoría cuando una empresa a cotizar tiene múltiples oficinas, plantas o sucursales físicas y virtuales.

El Anexo D (Informativo) de la norma ISO/IEC 27006-1:2022 se titula: "Directrices para los organismos de certificación que utilizan el muestreo de sitios en organizaciones multi-sitio".

Su propósito es regular bajo qué condiciones de ciberseguridad una casa certificadora puede aplicar fórmulas de muestreo (como la raíz cuadrada) para no tener que viajar o auditar el 100% de las sucursales físicas o virtuales de un cliente, protegiendo la integridad del esquema.

D.1 Generalidades

Establece que el muestreo de sitios en un Sistema de Gestión de la Seguridad de la Información (SGSI) es aceptable, pero debe ser abordado con extrema precaución. A diferencia de otros esquemas (como Calidad), la seguridad de la información de una sucursal remota puede poner en riesgo a toda la corporación, por lo que el muestreo debe estar estrictamente justificado mediante un enfoque basado en riesgos.

9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

D.2 Elegibilidad de las organizaciones para el muestreo (¿Quién califica?)

Para que una casa certificadora apruebe el muestreo y reduzca los sitios a auditar, la empresa cliente debe demostrar obligatoriamente tres condiciones de control centralizado:

-Gestión Centralizada: Un único equipo o rol (ej. el CISO) debe tener la autoridad legal y operativa para imponer políticas de seguridad en todas las sucursales.

-Un único SGSI: Debe existir un solo Análisis de Riesgos y una sola Declaración de Aplicabilidad (SoA) global. No se permite que cada sucursal decida qué controles de la ISO 27001 aplicar.

-Auditoría e informes unificados: La oficina central debe haber auditado internamente a todas las sucursales y haber realizado una Revisión por la Dirección consolidada antes de recibir a los auditores externos.

D.3 Metodologías de Muestreo (¿Cómo elegir las sedes?)

El anexo prohíbe que la selección de las sucursales sea 100% al azar. Exige un Muestreo No Aleatorio y Basado en Riesgos:

-El organismo de certificación debe elegir intencionalmente los sitios que presenten mayores amenazas (por ejemplo, sedes que manejen datos de clientes más sensibles, sucursales que hayan reportado incidentes o hackeos en el último año, o locaciones con alta rotación de personal de TI).

9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

D.4 Selección de la Muestra

Estratificación: Obliga a agrupar las sucursales por "tipos homogéneos" antes de aplicar la matemática. Si una empresa tiene 10 centros de datos y 50 oficinas de venta, se deben crear dos grupos (estratos) separados y calcular una muestra para cada grupo, ya que sus riesgos tecnológicos son completamente distintos.

Rotación en el tiempo: El diseño de la muestra debe garantizar que durante el ciclo de 3 años (Certificación + Vigilancia 1 + Vigilancia 2), las sucursales auditadas vayan rotando para que ningún sitio se quede en un "punto ciego" permanente.

D.5 Auditoría de los Sitios de la Muestra

Cuando el auditor llega a la sucursal seleccionada, el Anexo D le ordena enfocarse en:

-Interfaces y conexiones: Evaluar cómo se comunica esa sede con los servidores centrales.

-Cumplimiento local de la SoA: Verificar si los empleados de esa sucursal conocen y operan los controles tecnológicos (antivirus, políticas de escritorio limpio, control de accesos físicos) dictados por la oficina central.

D.6 Informes y Certificación

El informe final de la auditoría debe listar con total transparencia cuáles sitios fueron auditados físicamente/remotamente y cuáles quedaron exentos por muestreo. El alcance del certificado físico debe reflejar esta condición para no inducir a error al mercado.

9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

Diagrama de Flujo del Proceso del Anexo D

Para que el personal técnico de la casa certificadora aplique este anexo sin errores, el proceso lógico e instructivo de selección se estructura de la siguiente manera:

Filtro de Elegibilidad: Validar si la empresa tiene un SGSI centralizado, auditoría interna total y un SoA único. Si falla un elemento, se cancela el muestreo y se audita el 100% de los sitios.

Estratificación: Separar las sedes en grupos según su función tecnológica (ej. Centros de datos vs. Oficinas administrativas).

Cálculo Base: Aplicar la fórmula correspondiente (comúnmente alineada al documento normativo global IAF MD 1).

Selección por Riesgo: Asignar una parte de la muestra a los sitios con mayor índice de incidentes o criticidad de datos, y el resto de forma aleatoria.

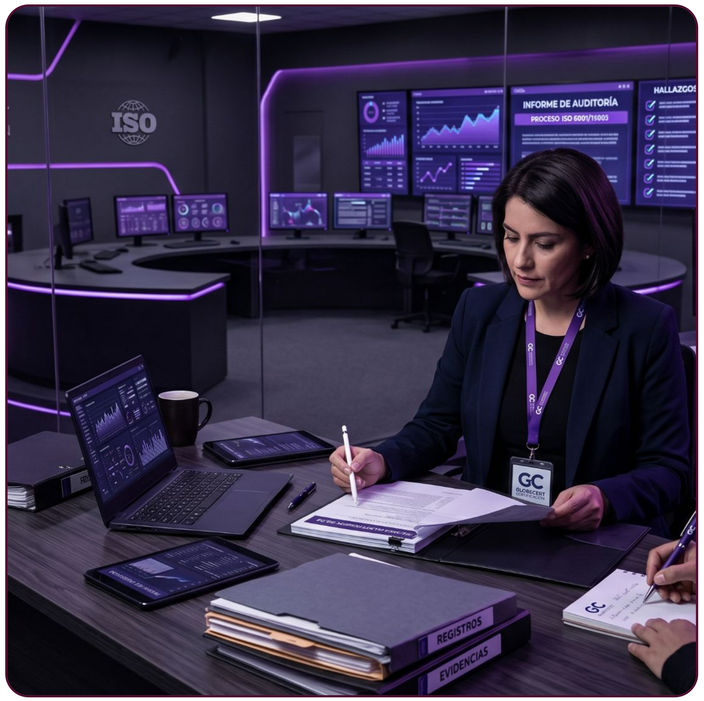
Diseño de Rotación: Registrar las sedes elegidas para asegurar que en los años de vigilancia (seguimientos) se visiten sucursales distintas.

9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

- **9.1.5. Muestreo de sitios múltiples (Multi-site sampling):** Esta cláusula define las reglas del juego para que un Organismo de Certificación (OC) pueda auditar una empresa que tiene varias sedes o sucursales utilizando una muestra, en lugar de visitarlas todas. Establece las condiciones estrictas que debe cumplir el cliente para ser apto y los factores de riesgo específicos de seguridad de la información que el OC debe ponderar para elegir esa muestra sin comprometer la confianza del Sistema de Gestión de la Seguridad de la Información (SGSI); Esta cláusula dicta si una empresa califica o no para que sus sucursales sean auditadas mediante "muestreo" (en lugar de ir a todas) activando el **Anexo D**.



9.1.5.1: Generalidades (General): Los requisitos de la norma ISO/IEC 17021-1, 9.1.5 se aplican. Además, se aplican los requisitos y la guía proporcionados en 9.1.5.2.

9.1.5.2: Sitios múltiples (Multiple sites): Núcleo operativo que desglosa los criterios técnicos de elegibilidad para el cliente y los procedimientos de control que debe ejecutar el Organismo de Certificación.

9.1.5.2.1 Criterios de elegibilidad del cliente: Cuando un cliente tiene un número de sitios que cumplen con los criterios de la letra a) a la c) a continuación, los organismos de certificación pueden considerar el uso de un enfoque basado en muestras para auditoría de sitios múltiples:

9. Requisitos relativos a los procesos

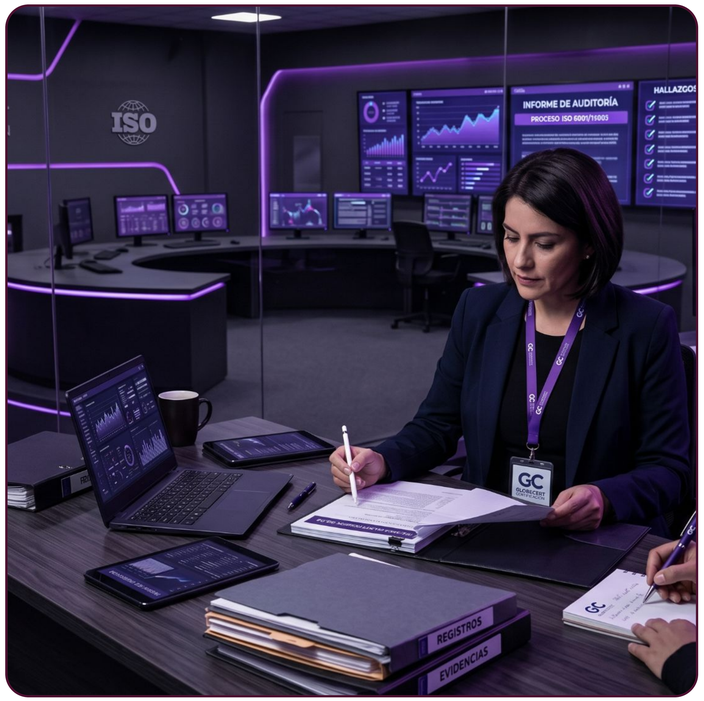
9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

a) todos los sitios operan bajo el mismo SGSI, el cual es administrado y auditado centralizadamente y está sujeto a una revisión por la dirección central;

b) todos los sitios están incluidos dentro del programa de auditoría interna del SGSI del cliente;

c) todos los sitios están incluidos dentro del programa de revisión por la dirección del SGSI del cliente.



9.1.5.2.2 Procedimientos del Organismo de Certificación: El organismo de certificación que desee utilizar un enfoque basado en muestras debe tener procedimientos implementados para asegurar lo siguiente:

a) La revisión inicial del contrato identifica, en la mayor medida posible, la diferencia entre los sitios, de modo que se determine un nivel adecuado de muestreo.

b) El organismo de certificación ha muestreado un número representativo de sitios, teniendo en cuenta:

-los resultados de las auditorías internas de la oficina central y de los sitios;

-los resultados de la revisión por la dirección;

-variaciones en el tamaño de los sitios;

9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

-variaciones en el propósito comercial de los sitios;

-complejidad de los sistemas de información en los diferentes sitios;

-variaciones en las prácticas de trabajo;

-variaciones en las actividades realizadas;

-variaciones en el diseño y operación de los controles;

-interacción potencial con sistemas de información críticos o sistemas de información que -procesan información sensible;

-cualquier requisito legal diferente;

-aspectos geográficos y culturales;

-situación de riesgo de los sitios;

-incidentes de seguridad de la información en sitios específicos.

c) Se selecciona una muestra representativa de todos los sitios dentro del alcance del SGSI del cliente; esta selección se basará en una combinación de muestreo selectivo (basado en riesgo) y muestreo aleatorio.

9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

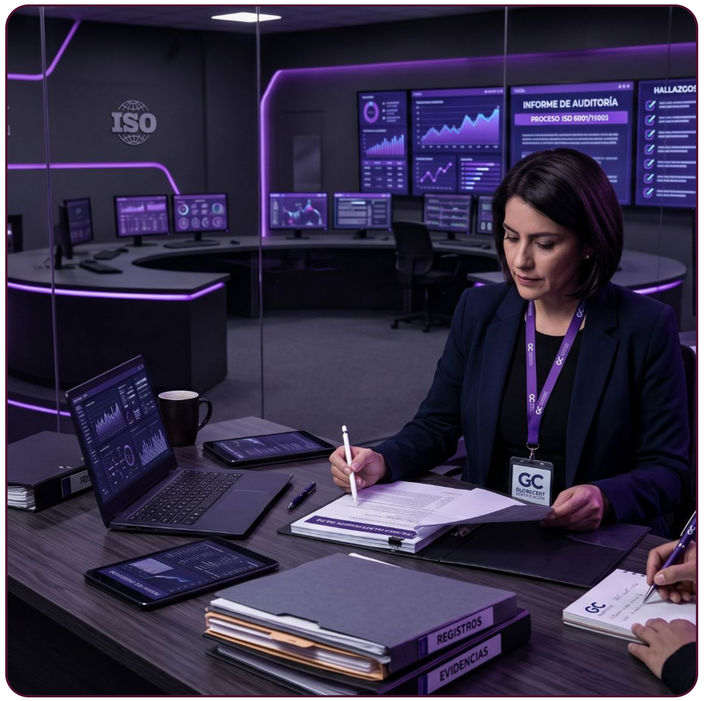
Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

- **9.1.6 Sistemas de gestión múltiples:** Esta sección especifica las reglas adicionales que un organismo de certificación debe aplicar cuando una organización auditada tiene integrados varios sistemas de gestión (por ejemplo, Calidad, Medio Ambiente o Continuidad del Negocio) junto con su Sistema de Gestión de la Seguridad de la Información (SGSI), regulando la aceptación de dicha documentación y la combinación de las auditorías.

9.1.6.1 Generalidades :Los requisitos de ISO/IEC 17021-1, 9.1.6 se aplican. Además, se aplican los requisitos y la orientación en 9.1.6.2 y 9.1.6.3.

9.1.6.2 Integración de la documentación del SGSI y de otros sistemas de gestión: El organismo de certificación puede aceptar documentación combinada (por ejemplo, para seguridad de la información, calidad, salud y seguridad, y medio ambiente), siempre que el SGSI pueda identificarse claramente junto con las interfaces apropiadas con los otros sistemas.

9.1.6.3 Auditorías combinadas de sistemas de gestión: La auditoría del SGSI se puede combinar con auditorías de otros sistemas de gestión, siempre que se pueda demostrar que la auditoría del SGSI cumple con todos los requisitos de este documento. En particular, esto incluye los requisitos de competencia para el equipo de auditoría establecidos en este documento.

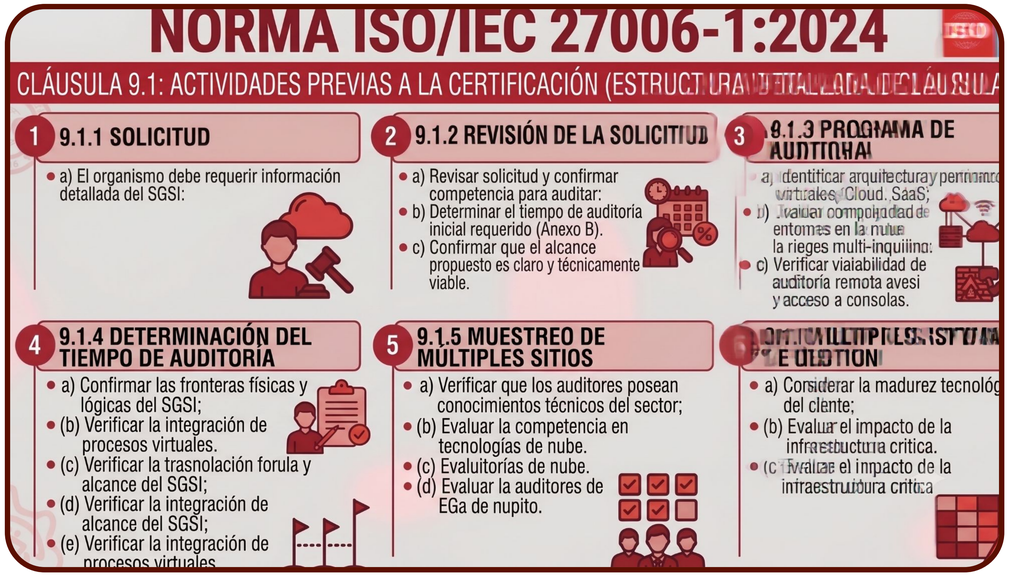


9. Requisitos relativos a los procesos

9.1 Actividades previas a la certificación

Regula el contacto inicial con el cliente, la recolección de datos y el diseño de la estrategia de evaluación.

Resumen: la cláusula 9.1 Norma los requisitos obligatorios de captura de información y análisis de riesgos previos a la contratación o planificación de la auditoría del SGSI. Introduce la obligatoriedad de evaluar el entorno técnico del cliente, sus activos críticos y la seguridad de las plataformas si se opta por auditorías virtuales. Asegura que el proceso de certificación empiece con un conocimiento profundo, transparente y cuantificable del alcance.



9. Requisitos relativos a los procesos

9.2 Planificación de las auditorías

Establece los preparativos específicos previos a la ejecución de la auditoría en campo.

Esta cláusula establece las reglas e instrucciones específicas que los organismos de certificación deben seguir al planificar las auditorías de un SGSI. Se enfoca en cómo determinar el tiempo que durará la auditoría, cómo seleccionar al equipo auditor adecuado y qué elementos de la organización del cliente deben ser considerados obligatoriamente durante el diseño del plan de auditoría.

Esta cláusula se divide formalmente en tres sub cláusulas principales (de la 9.2.1 a la 9.2.3), con requisitos muy específicos:

- **(IS 9.2.1) Determinación de los objetivos, alcance y criterios de la auditoría** Los requisitos de ISO/IEC 17021-1, 9.2 se aplican.

9. Requisitos relativos a los procesos

9.2 Planificación de las auditorías

Establece los preparativos específicos previos a la ejecución de la auditoría en campo.

9.2.1.1 Validación del Alcance del SGSI del Cliente: El organismo de certificación debe confirmar que el cliente ha definido el alcance de su SGSI de acuerdo con los requisitos de la norma ISO/IEC 27001. El organismo de certificación debe verificar que el alcance propuesto sea coherente con el contexto de la organización, sus interfaces y dependencias, y que incluya todas las actividades y procesos relevantes que impactan la seguridad de la información dentro de esos límites establecidos.

9.2.1.2 Consideración de Controles Excluidos y Declaración de Aplicabilidad (SoA): El organismo de certificación debe asegurarse de que los criterios de auditoría incluya la Declaración de Aplicabilidad (SoA) del cliente. Durante la determinación de los objetivos y criterios, se debe evaluar la justificación de cualquier exclusión de controles del Anexo A de la norma ISO/IEC 27001, verificando que dichas exclusiones no comprometan la capacidad ni la responsabilidad de la organización para proporcionar seguridad de la información según sus evaluaciones de riesgos.

9.2.1.3 Estructuras Multi-sitio e Infraestructuras Virtuales: Cuando el alcance de la auditoría involucra múltiples ubicaciones físicas o entornos virtuales (como nubes públicas o privadas), el organismo de certificación debe definir objetivos y criterios específicos que abarquen el control del SGSI sobre estas infraestructuras descentralizadas. Se debe asegurar la trazabilidad de los flujos de información y los límites de control entre los distintos sitios incluidos en la solicitud de certificación.

9. Requisitos relativos a los procesos

9.2 Planificación de las auditorías

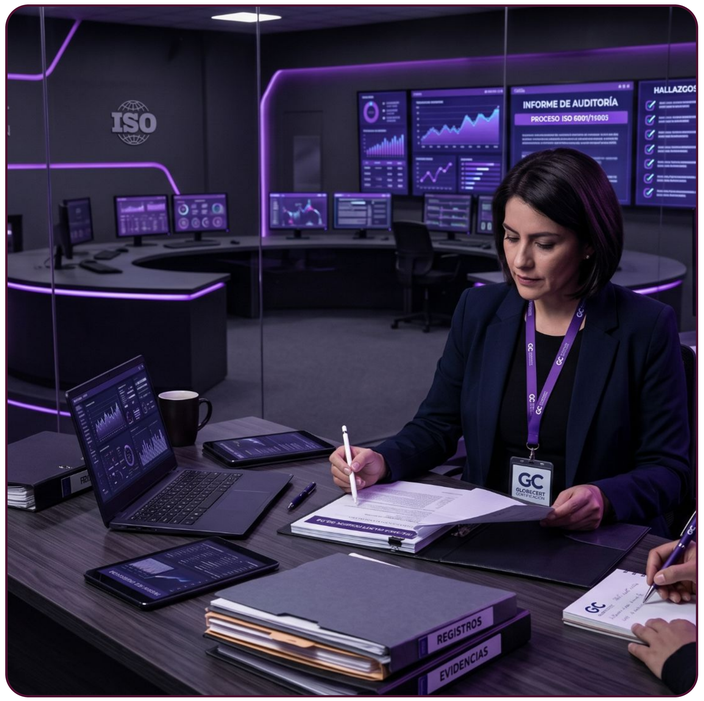
Establece los preparativos específicos previos a la ejecución de la auditoría en campo.

- **(IS 9.2.2) Selección y asignación del equipo auditor**

  La norma estipula que al seleccionar el equipo auditor, el organismo de certificación debe asegurar que el equipo disponga de la competencia técnica colectiva para el alcance de la certificación. Esto incluye la comprensión de la tecnología de la información, la seguridad de la información y los procesos de negocio del cliente. Se debe designar formalmente a un auditor líder del equipo.

  9.2.2.1 Competencia del Equipo en el Sector Específico: El equipo de auditoría debe poseer conocimientos específicos del sector en el que opera el cliente. Esto implica comprender los riesgos típicos de seguridad de la información asociados a ese sector, las regulaciones legales y normativas aplicables a la industria, y los procesos operativos comunes. Si el equipo no cuenta con este conocimiento internamente, se debe recurrir a expertos técnicos.

  9.2.2.2 Roles y Supervisión de Auditores en Formación: Los auditores en formación (conocidos también como auditores en prácticas) pueden ser incluidos en el equipo de auditoría, pero no deben auditar de manera independiente. Deben estar bajo la supervisión constante y directa de un auditor calificado. Sus actividades y hallazgos no se consideran válidos para la toma de decisiones a menos que sean refrendados por el auditor supervisor.



9. Requisitos relativos a los procesos

9.2 Planificación de las auditorías

Establece los preparativos específicos previos a la ejecución de la auditoría en campo.

- **(IS 9.2.3) Plan de auditoría (Audit plan):** Esta cláusula norma los requisitos específicos del SGSI aplicados al diseño del plan de auditoría. Establece consideraciones precisas sobre los controles de seguridad seleccionados y las reglas técnicas para auditorías remotas. Su objetivo es garantizar la eficiencia operativa sin comprometer el rigor evaluativo.

9.2.3.1 Generalidades :Los requisitos de ISO/IEC 17021-1, 9.2.3 se aplican. Además, se aplican los requisitos y la orientación en 9.2.3.2. y 9.2.3.3.

9.2.3.2 Disposiciones generales: El plan de auditoría para las auditorías de SGSI se crea teniendo en cuenta los controles de seguridad de la información especificados.

9.2.3.3 Técnicas de auditoría remota: El objetivo de las técnicas de auditoría remota debe ser aumentar la eficacia y la eficiencia de la auditoría y respaldar la integridad del proceso de auditoría. El plan de auditoría debe hacer referencia a las herramientas utilizadas para asistir con la auditoría remota.

💡 La versión 2024 te da total libertad de auditar en remoto, pero con una condición: tienes que escribir en el plan qué herramientas vas a usar (Teams, Zoom, etc). No se vale improvisar la tecnología sobre la marcha ni usar canales inseguros para auditar.

9. Requisitos relativos a los procesos

9.2 Planificación de las auditorías

Establece los preparativos específicos previos a la ejecución de la auditoría en campo.

Resumen: Regula los criterios obligatorios para planificar el tiempo y el alcance de las auditorías de certificación de seguridad de la información. Define cómo calcular los días de auditoría basándose en la complejidad del cliente y la efectividad de sus procesos. Asegura que el plan de auditoría cubra todos los frentes críticos del SGSI sin dejar cabos sueltos.

9. Requisitos relativos a los procesos

9.3 Certificación inicial

Define las fases obligatorias para organizaciones que buscan certificarse por primera vez.

Esta sección de la norma establece los requisitos adicionales específicos y obligatorios que un Organismo de Certificación (OC) debe aplicar al ejecutar el proceso de auditoría de certificación inicial para un Sistema de Gestión de la Seguridad de la Información (SGSI). Su objetivo es complementar las directrices generales de auditoría, enfocándose en la recopilación documental crítica y en la evaluación del diseño y efectividad del sistema de seguridad.

- **9.3.1 Generalidades:** Los requisitos y directrices de la norma ISO/IEC 17021-1 9.3 se aplican. Además, se aplicarán los requisitos y directrices establecidos en la cláusula 9.3.2.

(IS 9.3.2) Auditoría de certificación inicial: En esta etapa de la auditoría, el organismo de certificación debe obtener documentación relativa al diseño del SGSI, que abarque la documentación prevista en la norma ISO/IEC 27001.

Como mínimo, el cliente debe proporcionar la siguiente información durante la Etapa 1 del proceso de auditoría de certificación:

a) Información general sobre el SGSI y las actividades que abarca;

b) Una copia de la documentación requerida del SGSI especificada en la norma ISO/IEC 27001 y, cuando sea necesario, otra documentación relacionada.

9. Requisitos relativos a los procesos

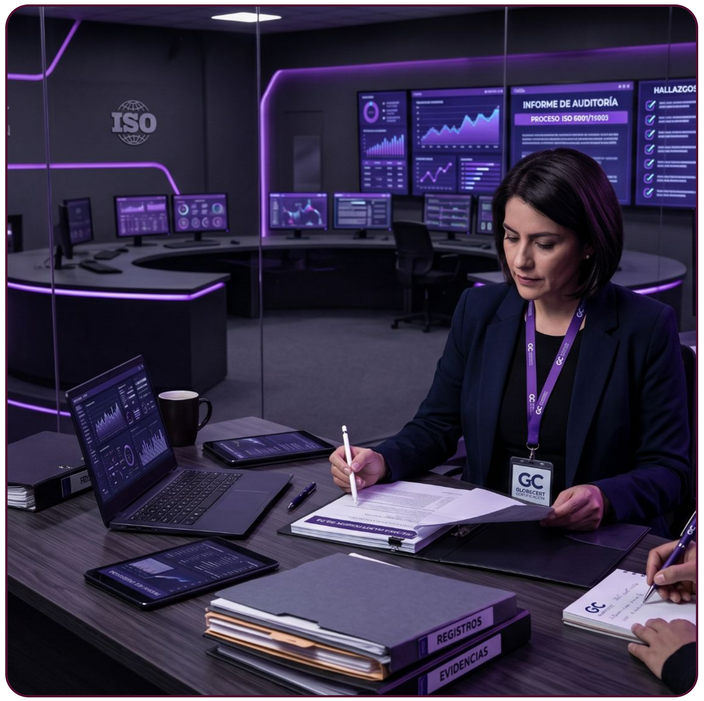
9.3 Certificación inicial

Define las fases obligatorias para organizaciones que buscan certificarse por primera vez.

9.3.2.2 Etapa 2 (Stage 2): Durante la Etapa 2 de la auditoría de certificación inicial, el organismo de certificación debe evaluar la implementación y la eficacia del SGSI del cliente en el sitio o mediante técnicas de auditoría a distancia de acuerdo con los requisitos aplicables. El organismo de certificación debe verificar que los objetivos de control y los controles de la Declaración de Aplicabilidad (SoA) estén basados en el proceso de evaluación y tratamiento de riesgos de seguridad de la información del cliente, y que estén efectivamente implementados.

9.3.2.3 Auditoría de Organizaciones Virtuales / Infraestructura Cloud: Cuando los procesos del cliente ocurren en infraestructuras virtuales (nubes públicas, plataformas SaaS, entornos híbridos o teletrabajo masivo), la subcláusula dicta que estos entornos virtuales deben ser auditados de la misma forma que una sede física.

💡 El organismo debe justificar en sus registros técnicos cómo se inspeccionó la seguridad lógica de esos activos a distancia, eliminando el antiguo límite rígido del 30% para auditorías remotas, pero incrementando la exigencia de verificación del gobierno de la nube.



9. Requisitos relativos a los procesos

9.3 Certificación inicial

Define las fases obligatorias para organizaciones que buscan certificarse por primera vez.

Resumen: La cláusula regula las exigencias técnicas para planificar y ejecutar las auditorías de certificación inicial de un SGSI. Divide el proceso en dos etapas críticas para garantizar que el organismo recopila la documentación de diseño y verifique la implementación real de los controles. Asegura que ningún certificado se emita sin validar rigurosamente la Declaración de Aplicabilidad (SoA) y la gestión de riesgos.

9. Requisitos relativos a los procesos

9.4 Realización de las auditorías

Describe las reglas metodológicas y de conducta que el equipo auditor debe seguir durante cualquier auditoría del ciclo.

Esta sección define las reglas específicas de juego y los criterios obligatorios que los organismos de certificación deben cumplir durante la ejecución de las auditorías de un SGSI (ISO/IEC 27001). Se enfoca primordialmente en la aplicación del muestreo de controles (Anexo A / Anexo E de la 27006-1) y la validez formal del uso de técnicas de auditoría remota, asegurando la transparencia y la rigurosidad metodológica del proceso de revisión.

En el texto normativo oficial, esta cláusula es una de las más detalladas y se divide formalmente en nueve sub cláusulas principales (de la 9.4.1 a la 9.4.3):

- **9.4.1 Generalidades:** Los requisitos establecidos en la norma ISO/IEC 17021-1 9.4 se aplican. Además, se aplican los siguientes requisitos específicos del SGSI y los listados en 9.4.2 y 9.4.3:

  -El equipo auditor debe auditar el SGSI de la organización cliente frente a los criterios de auditoría aplicables.

  -El equipo auditor debe verificar que la organización cliente haya definido e implementado un proceso de tratamiento de riesgos de seguridad de la información adecuado y que los controles seleccionados en la Declaración de Aplicabilidad (SoA) se implementen de manera eficaz.

  -El equipo auditor debe recopilar evidencia para verificar la implementación y eficacia de los controles de seguridad de la información.

9. Requisitos relativos a los procesos

9.4 Realización de las auditorías

Describe las reglas metodológicas y de conducta que el equipo auditor debe seguir durante cualquier auditoría del ciclo.

- **(IS 9.4.2) Elementos de auditoría específicos del SGSI:** El equipo auditor debe auditar los elementos específicos del SGSI que incluyen:

  a) La Declaración de Aplicabilidad (SoA), que contenga todos los controles necesarios en el proceso de tratamiento de riesgos y las justificaciones para las exclusiones;

  b) La correspondencia entre los controles implementados por la organización cliente y los resultados del proceso de evaluación y tratamiento de riesgos de seguridad de la información;

  c) La evidencia de la efectividad operativa de los controles implementados a través del muestreo adecuado de registros, observaciones y entrevistas.

  Esta cláusula exige que el organismo de certificación recopile y registre evidencias claras sobre la efectividad de los controles implementados por el cliente. Obliga a los auditores a utilizar el **Anexo E** como la guía técnica de referencia para saber qué preguntar, qué observar y qué probar al evaluar la Declaración de Aplicabilidad (SoA).

9. Requisitos relativos a los procesos

9.4 Realización de las auditorías
Describe las reglas metodológicas y de conducta que el equipo auditor debe seguir durante cualquier auditoría del ciclo.

📌 El Anexo E (Informativo) es una de las adiciones más significativas en la versión actual de la norma ISO/IEC 27006-1:2022. Lleva por título "Directrices para auditar los controles del SGSI" (Guidance for auditing ISMS controls).

Desarrollo del Anexo E: Guía para la Evaluación de Controles

El propósito del Anexo E es evitar que las auditorías de ISO 27001 sean meramente documentales (revisar que existan políticas firmadas). El anexo proporciona directrices técnicas para que el auditor evalúe la eficacia operativa de los controles bajo la nueva estructura de 4 pilares:

1. Controles Organizacionales (Cláusula 5 de ISO 27001)

Orienta al auditor sobre cómo evaluar la gobernanza de la seguridad. El Anexo E guía la revisión de elementos como:

-Políticas y directrices: Cómo comprobar que las políticas de seguridad están realmente integradas en la operación diaria y no solo guardadas en un PDF.

-Inteligencia de amenazas: Cómo auditar si la organización analiza activamente el entorno para detectar nuevas amenazas cibernéticas y si adapta sus controles en consecuencia.

-Seguridad en la cadena de suministro: Criterios para auditar cómo la empresa evalúa y supervisa el riesgo de sus proveedores y servicios en la nube (Cloud Providers).

9. Requisitos relativos a los procesos

9.4 Realización de las auditorías
Describe las reglas metodológicas y de conducta que el equipo auditor debe seguir durante cualquier auditoría del ciclo.

2. Controles de Personas (Cláusula 6 de ISO 27001)

Se enfoca en el factor humano antes, durante y después de la contratación. El anexo indica cómo verificar:

-Cultura y concientización: Técnicas para evaluar si los empleados realmente entienden los riesgos de ingeniería social (Phishing) mediante muestreos de entrevistas o resultados de simulacros internos.

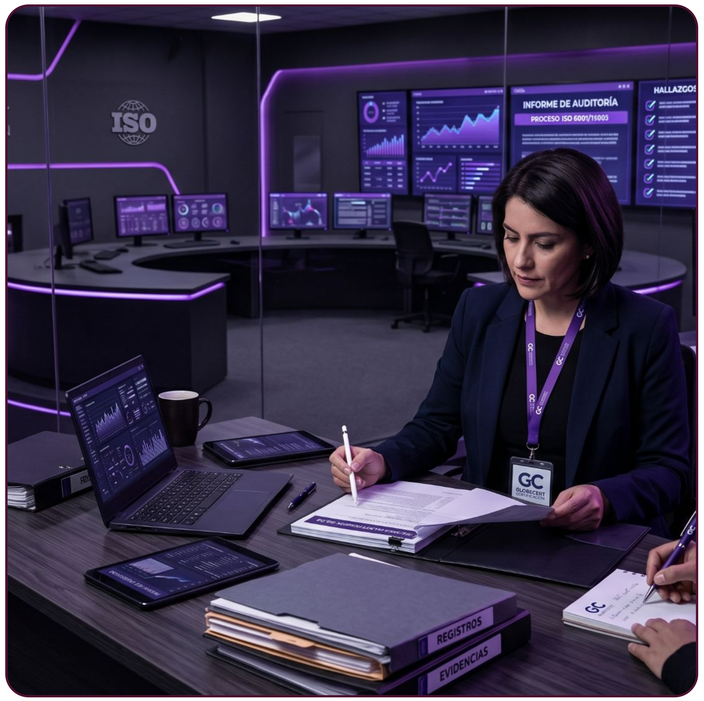
-Trabajo remoto: Pautas para auditar la seguridad de los empleados que trabajan desde casa (uso de redes domésticas, cifrado de equipos, manejo de información confidencial en entornos familiares).

3. Controles Físicos (Cláusula 7 de ISO 27001)

Establece las directrices para auditar el perímetro y las instalaciones donde residen los activos de información:

-Seguridad física: Cómo inspeccionar barreras, sistemas de control de acceso biométrico o tarjetas, y circuitos cerrados de televisión (CCTV).

-Seguridad de los activos e infraestructura de soporte: Guías para revisar el mantenimiento de plantas de energía redundante, sistemas de aire acondicionado en Centros de Datos y la protección del cableado de red.



9. Requisitos relativos a los procesos

9.4 Realización de las auditorías
Describe las reglas metodológicas y de conducta que el equipo auditor debe seguir durante cualquier auditoría del ciclo.

4. Controles Tecnológicos (Cláusula 8 de ISO 27001)

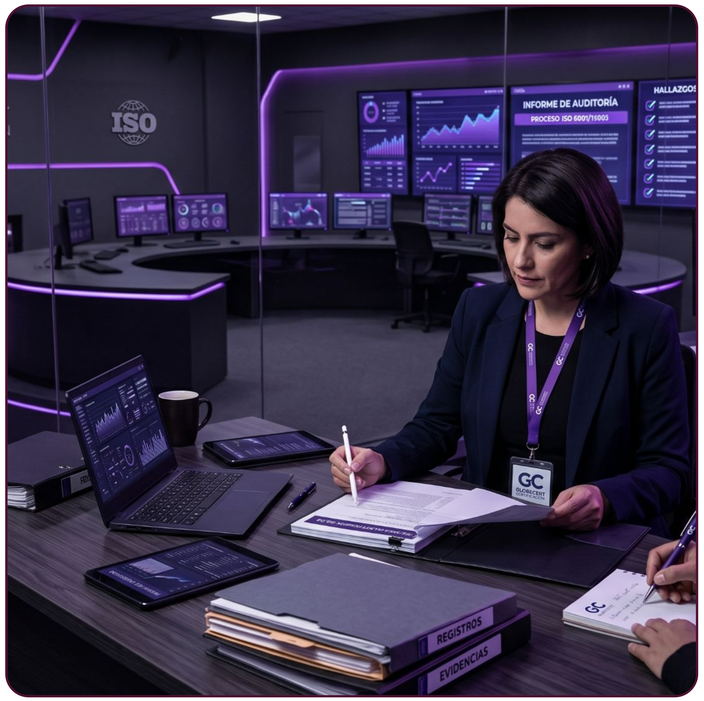
Es la sección más técnica y profunda del anexo. Proporciona pautas detalladas para auditar la infraestructura digital:

-Gestión de identidades y accesos (IAM): Cómo revisar las configuraciones de privilegios, autenticación de doble factor (2FA) y el ciclo de vida de las cuentas de usuario.

-Seguridad en el desarrollo de software: Criterios para auditar si la empresa programa de forma segura (pruebas estáticas/dinámicas de código, gestión de vulnerabilidades en librerías de terceros).

-Cifrado y criptografía: Cómo constatar que las llaves criptográficas se gestionan de forma segura y que los datos sensibles están protegidos tanto en tránsito como en reposo.

-Respaldo y continuidad de TI: Cómo auditar la efectividad real de las pruebas de restauración de backups y planes de recuperación ante desastres (DRP).



9. Requisitos relativos a los procesos

9.4 Realización de las auditorías

Describe las reglas metodológicas y de conducta que el equipo auditor debe seguir durante cualquier auditoría del ciclo.

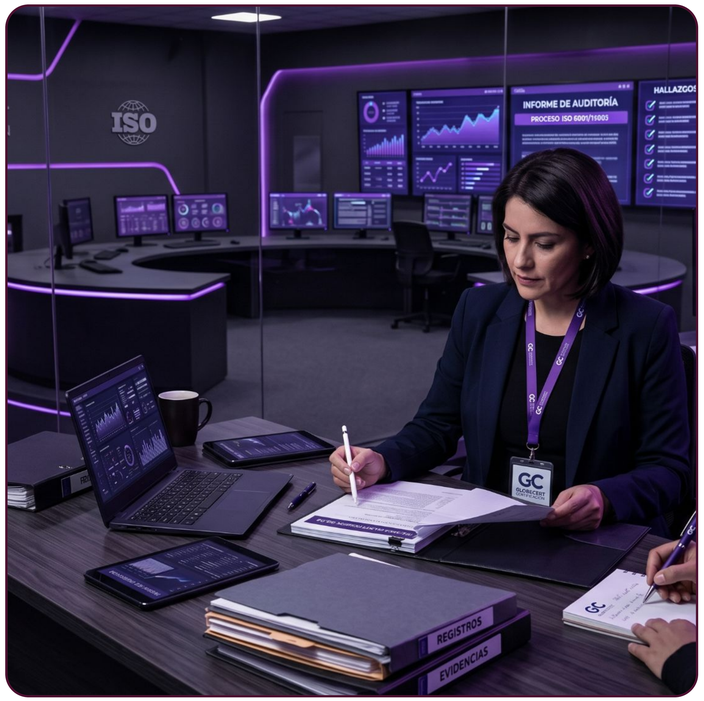
- **(IS 9.4.3) Informe de auditoría:** El informe de auditoría debe proporcionar un estado claro de la conformidad del SGSI y debe incluir adicionalmente:

  a) Una descripción del alcance de la auditoría y de los límites del SGSI de la organización cliente;

  b) Las conclusiones de la auditoría sobre la idoneidad, adecuación y efectividad del SGSI;

  c) Un resumen detallado de los controles del SGSI que fueron muestreados y validados durante la auditoría;

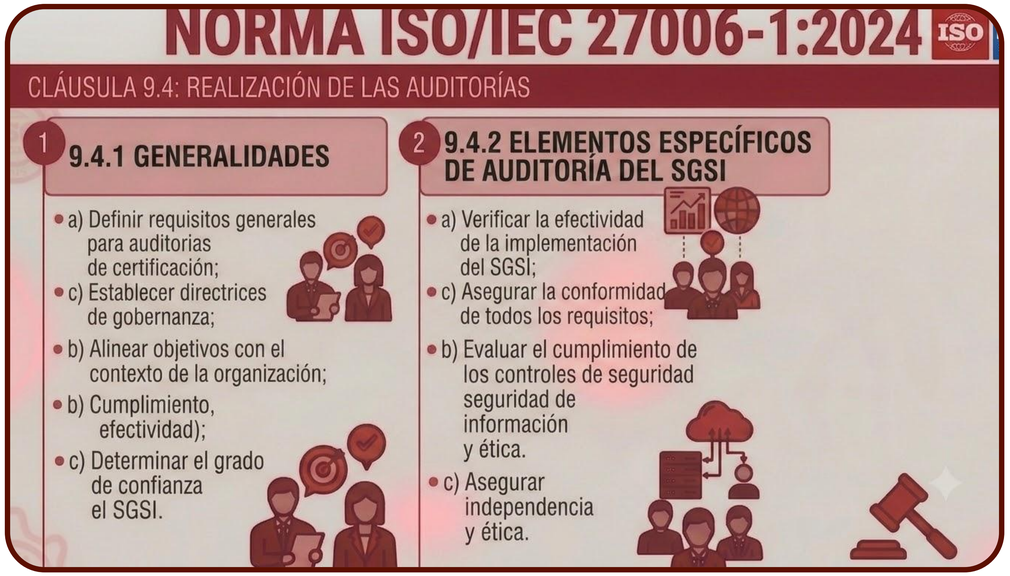
  d) El alcance y la efectividad percibida de cualquier técnica de auditoría remota utilizada, justificando su aplicación en el informe técnico.



9. Requisitos relativos a los procesos

9.4 Realización de las auditorías
Describe las reglas metodológicas y de conducta que el equipo auditor debe seguir durante cualquier auditoría del ciclo.

Resumen: Esta cláusula norma de forma estricta cómo se deben ejecutar las auditorías de certificación del SGSI, obligando al equipo auditor a evaluar detalladamente la eficacia de los controles seleccionados por la organización. Asimismo, introduce lineamientos precisos sobre la transparencia y justificación que se deben reportar al hacer uso de metodologías y técnicas de auditoría remota.

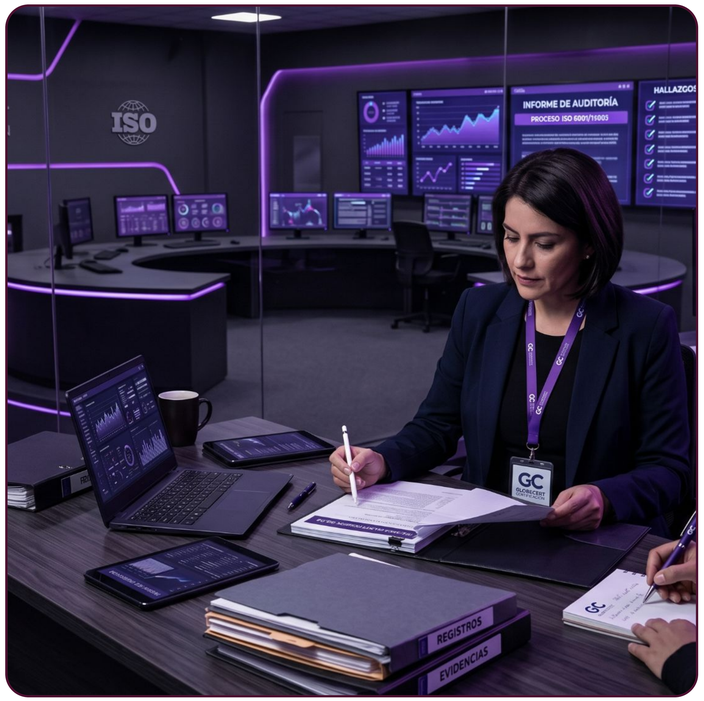


9. Requisitos relativos a los procesos

9.5 Decisión de certificación

El núcleo que garantiza la imparcialidad del proceso.

Los requisitos establecidos en la norma ISO/IEC 17021-1:2015, 9.5



💡 Recuerda, Si una cláusula se ejecuta de manera idéntica y estándar, el documento lo declara directamente en su cuerpo principal (indicando que aplican los requisitos de la ISO/IEC 17021-1:2015) y se omite por completo de cualquier anexo de análisis para evitar engrosar el texto de forma redundante.

9. Requisitos relativos a los procesos

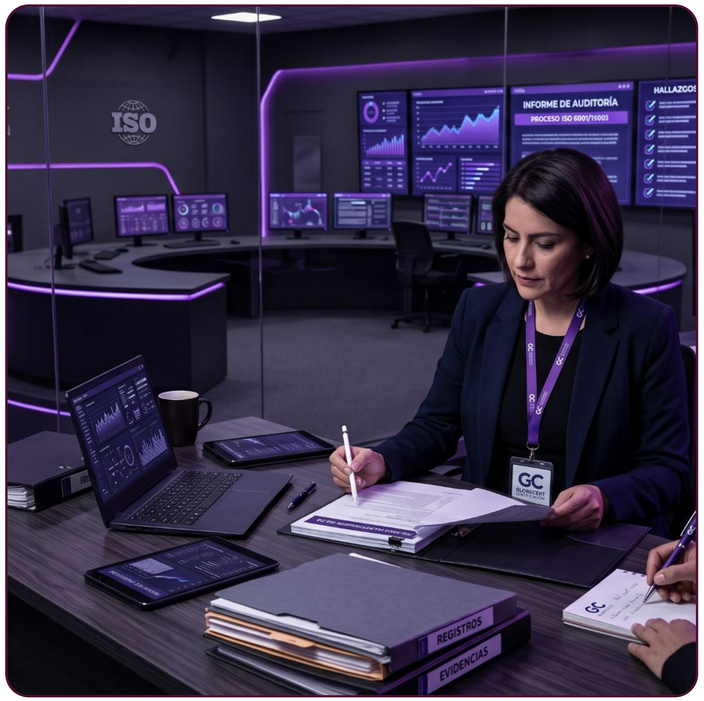
9.6 Mantenimiento de la certificación

Regula el seguimiento obligatorio post-certificación.

- **9.6.1 General:** Los requisitos establecidos en la norma ISO/IEC 17021-1:2015, 9.6

- **9.6.2 General: Actividades de vigilancia:** Este apartado regula cómo los organismos de certificación deben planificar y ejecutar las auditorías de vigilancia (seguimientos anuales) y las auditorías de recertificación (cada 3 años). Su objetivo principal como requerimiento IS (Information Security) es garantizar que la efectividad de la seguridad de la información sea evaluada de forma continua y completa, evitando que los auditores revisen siempre los mismos temas o dejen controles críticos sin evaluar.

  9.6.2.1 Componente General (Vínculo con ISO/IEC 17021-1): El primer sub-numeral actúa como el puente de adopción. Establece que los aspectos procedimentales básicos (frecuencias, tiempos máximos para realizar las visitas, gestión de las fechas de vencimiento del certificado y la estructura básica del plan de auditoría de mantenimiento) deben seguir estrictamente lo definido en la norma matriz ISO/IEC 17021-1:2015.



9. Requisitos relativos a los procesos

9.6 Mantenimiento de la certificación

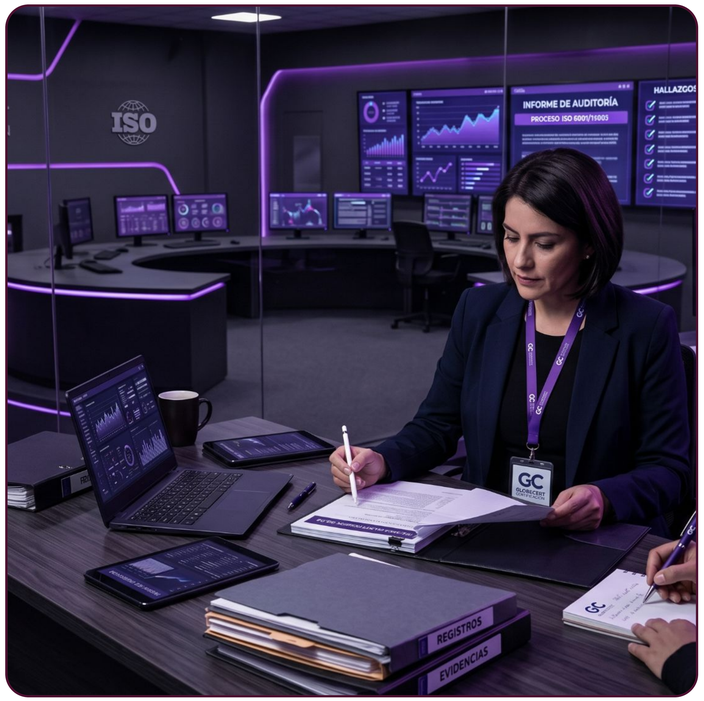
Regula el seguimiento obligatorio post-certificación.

(IS 9.6.2.2) Requisitos Especiales IS para Auditorías de Vigilancia (Mantenimiento): La norma exige que las auditorías de seguimiento anuales no sean genéricas y obliga a que incluyan de manera mandatoria la revisión de:

-Elementos Core del SGSI: Se debe verificar el estado y actualización de la política de seguridad, la efectividad del proceso continuo de Apreciación y Tratamiento de Riesgos, y las acciones tomadas ante incidentes de seguridad reales que haya sufrido la empresa en el último año.

-Manejo de Cambios Significativos: El auditor debe revisar si el cliente modificó su infraestructura, si migró servicios a nuevas nubes, si cambió de proveedores críticos o si hubo reformas legales que afecten su cumplimiento. Cualquier cambio de este tipo obliga a evaluar cómo impactó al SGSI.

-El Principio del Muestreo Representativo (Ciclo de 3 años): Esta es la regla técnica más importante. El organismo de certificación debe diseñar un plan de muestreo de controles a lo largo de los seguimientos de tal manera que, al finalizar el ciclo de certificación (Año 1 y Año 2 de vigilancia), se hayan auditado obligatoriamente la totalidad de los controles declarados como aplicables en la Declaración de Aplicabilidad (SoA). No se permite dejar controles sin verificar durante el ciclo de vida del certificado.



9. Requisitos relativos a los procesos

9.6 Mantenimiento de la certificación

Regula el seguimiento obligatorio post-certificación.

(IS 9.6.2.3) Requisitos Especiales IS para la Auditoría de Recertificación (Año 3): Cuando el certificado está por expirar y se ejecuta la auditoría de recertificación para renovarlo por otros 3 años, el requerimiento IS exige que la evaluación sea integral y profunda, actuando casi como una auditoría inicial (Fase 2). Los auditores deben obligatoriamente constatar:

-Eficacia global e interconexión: No basta con revisar controles aislados; se debe comprobar que el SGSI funciona como un ecosistema donde la gestión de riesgos realmente dicta qué controles se operan y que la dirección está al tanto del desempeño real de la seguridad.

-Revisión completa de la Declaración de Aplicabilidad (SoA): Se debe validar la vigencia de la versión actual del SoA frente a las amenazas emergentes del entorno del cliente, confirmando que las exclusiones de controles sigan estando técnicamente justificadas.

-Historial de mejora continua: Se evalúa el archivo de los 3 años anteriores de auditorías internas, revisiones por la dirección y el cierre efectivo de cualquier vulnerabilidad o no conformidad del pasado.

9. Requisitos relativos a los procesos

9.6 Mantenimiento de la certificación

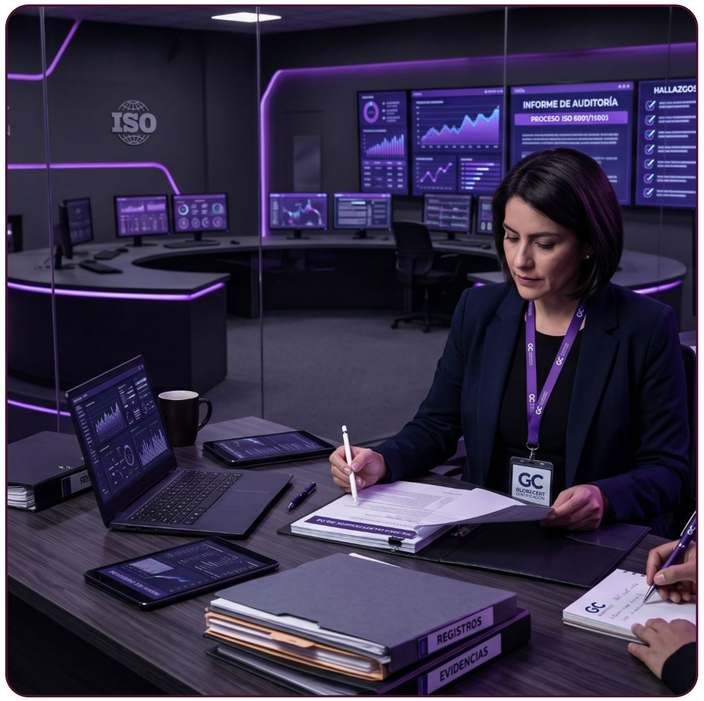
Regula el seguimiento obligatorio post-certificación.

- **9.6.3 Auditoría de Recertificación:** evalúa los requisitos para renovar el certificado cada 3 años.

  Validación de la eficacia global del SGSI: El organismo de certificación debe confirmar que el sistema de gestión funciona de manera madura e integrada. Esto implica demostrar que los resultados de las auditorías internas y las revisiones por la dirección a lo largo de los 3 años han servido para mejorar la seguridad real de la empresa.

  Revisión exhaustiva del SoA (Declaración de Aplicabilidad): Se exige al auditor verificar detalladamente que la versión actual del SoA responde fielmente al panorama de riesgos actual de la organización. El auditor debe validar que cualquier exclusión de controles siga estando técnicamente justificada y documentada.

  Muestreo de controles: Al ser una recertificación, la intensidad de la revisión de los controles del Anexo A de la ISO 27001 es mucho mayor que en un seguimiento anual; se debe asegurar que no queden "puntos ciegos" tecnológicos o de procesos antes de emitir el nuevo certificado por otros 3 años.



9. Requisitos relativos a los procesos

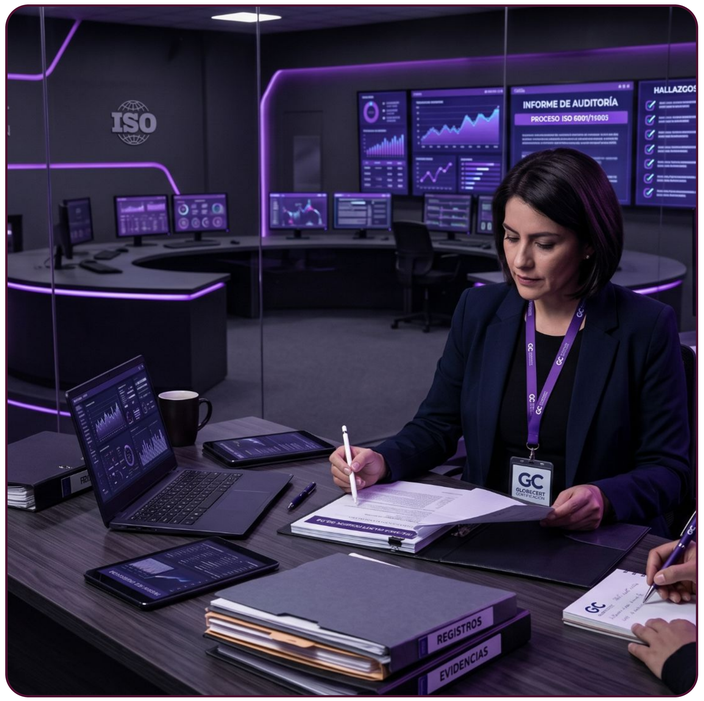
9.6 Mantenimiento de la certificación

Regula el seguimiento obligatorio post-certificación.

- **9.6.4 Auditorías Especiales:** Este apartado regula las evaluaciones fuera del ciclo normal, divididas en dos escenarios: extensiones de alcance solicitadas por el cliente o auditorías con previo aviso corto.

  Extensiones de Alcance (Ampliaciones): Si la empresa quiere certificar un nuevo servicio tecnológico, una nueva app o un nuevo centro de datos, la norma IS prohíbe añadirlo administrativamente. Exige realizar una auditoría especial para evaluar el impacto en el análisis de riesgos existente y verificar si la ampliación obliga a activar controles del Anexo A que la empresa antes tenía excluidos.

  Auditorías con Previo Aviso Corto (Short-Notice Audits): Este es un control de emergencia. La norma IS exige que la casa certificadora tenga la facultad de presentarse a auditar de forma imprevista o con pocos días de aviso si se entera de que el cliente sufrió un incidente de seguridad de la información grave (como una fuga masiva de datos, un hackeo crítico o un ataque de ransomware que afecte la integridad del SGSI). El objetivo de esta auditoría especial es investigar si el SGSI de la empresa falló, si los controles eran ineficaces o si la organización ocultó riesgos.



9. Requisitos relativos a los procesos

9.6 Mantenimiento de la certificación

Regula el seguimiento obligatorio post-certificación.

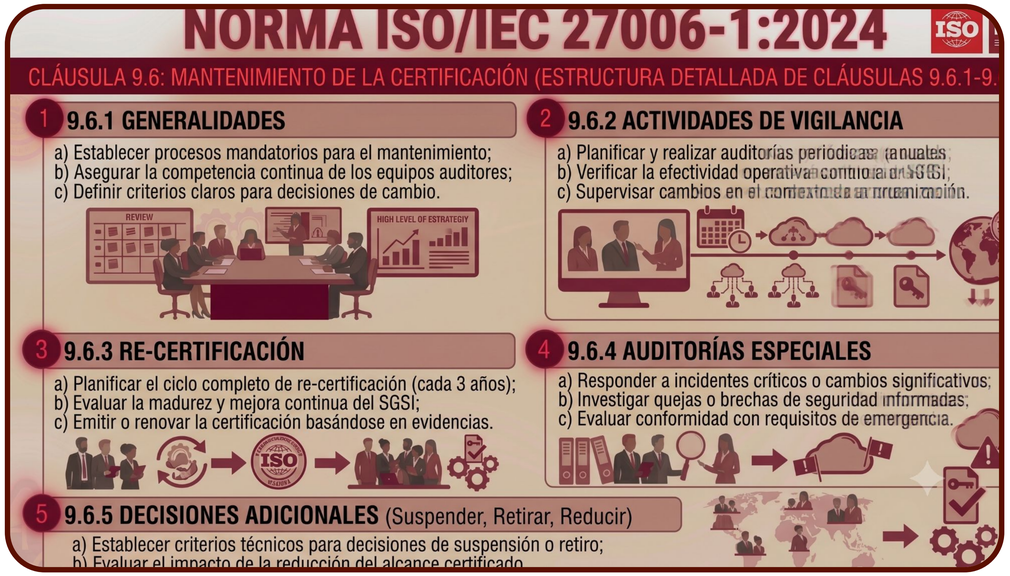
- **9.6.5 Suspensión, Retirada o Reducción del Alcance:** Los requisitos de la norma ISO/IEC 17021-1:2015, 9.6.5 deben aplicarse.

9. Requisitos relativos a los procesos

9.6 Mantenimiento de la certificación

Regula el seguimiento obligatorio post-certificación.

Resumen: Si un organismo de certificación no cuenta con una matriz o un plan de seguimiento que demuestre de forma explícita cómo va a "repartir" la revisión de los más de 90 controles de la ISO 27001 (versión 2024) entre las auditorías de vigilancia del Año 1 y Año 2 para asegurar la cobertura del 100% del SoA, estará cometiendo un incumplimiento directo contra este requisito IS y podría perder su acreditación.



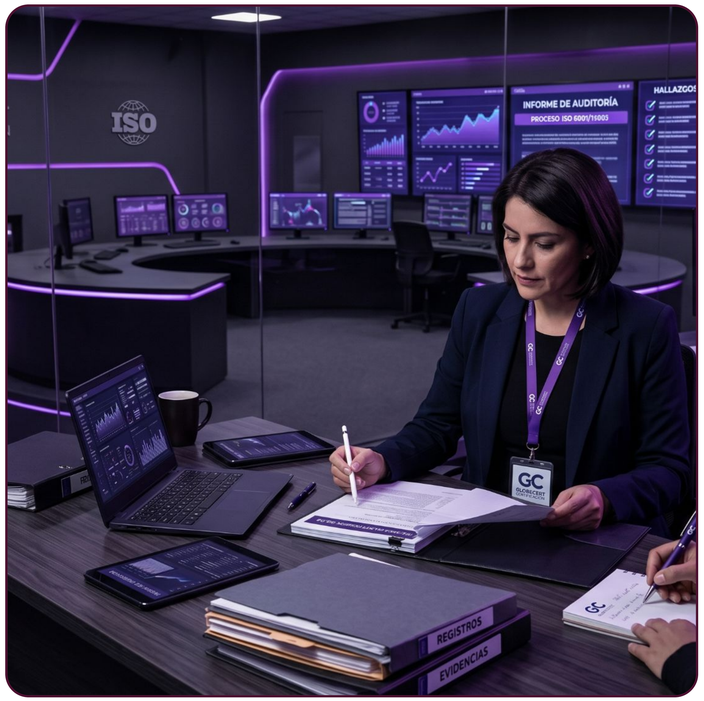
9. Requisitos relativos a los procesos

9.7 Apelaciones

Establece el proceso para que los clientes soliciten la reconsideración de una decisión adversa tomada por el organismo de certificación.

El organismo de certificación debe aplicar los requisitos de la norma ISO/IEC 17021-1:2015, cláusula 9.7.

💡 Recuerda, Si una cláusula se ejecuta de manera idéntica y estándar, el documento lo declara directamente en su cuerpo principal (indicando que aplican los requisitos de la ISO/IEC 17021-1:2015) y se omite por completo de cualquier anexo de análisis para evitar engrosar el texto de forma redundante.



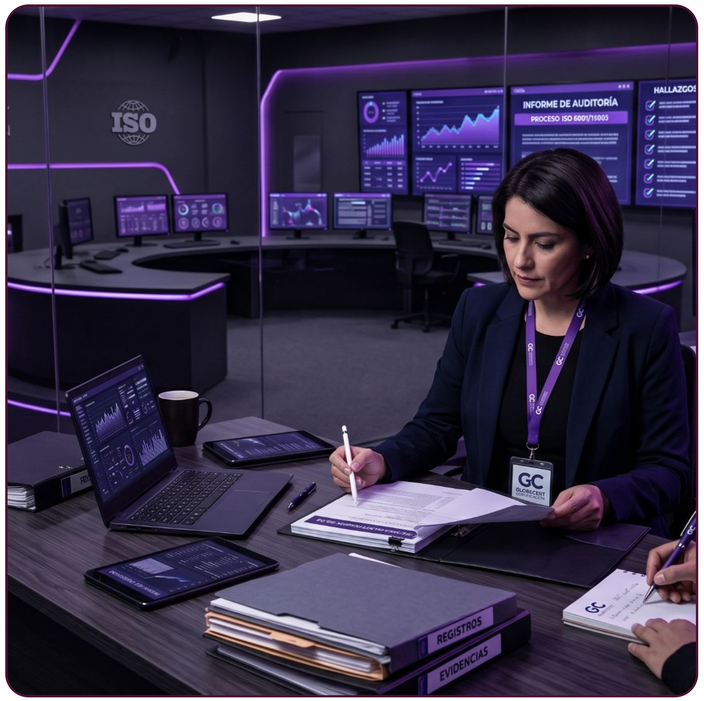
9. Requisitos relativos a los procesos

9.8 Quejas

Regula la recepción, validación e investigación de expresiones de insatisfacción sobre las actividades del organismo o sus certificados.

El organismo de certificación debe aplicar los requisitos especificados en la Norma ISO/IEC 17021-1:2015, cláusula 9.8.

💡 Recuerda, Si una cláusula se ejecuta de manera idéntica y estándar, el documento lo declara directamente en su cuerpo principal (indicando que aplican los requisitos de la ISO/IEC 17021-1:2015) y se omite por completo de cualquier anexo de análisis para evitar engrosar el texto de forma redundante.



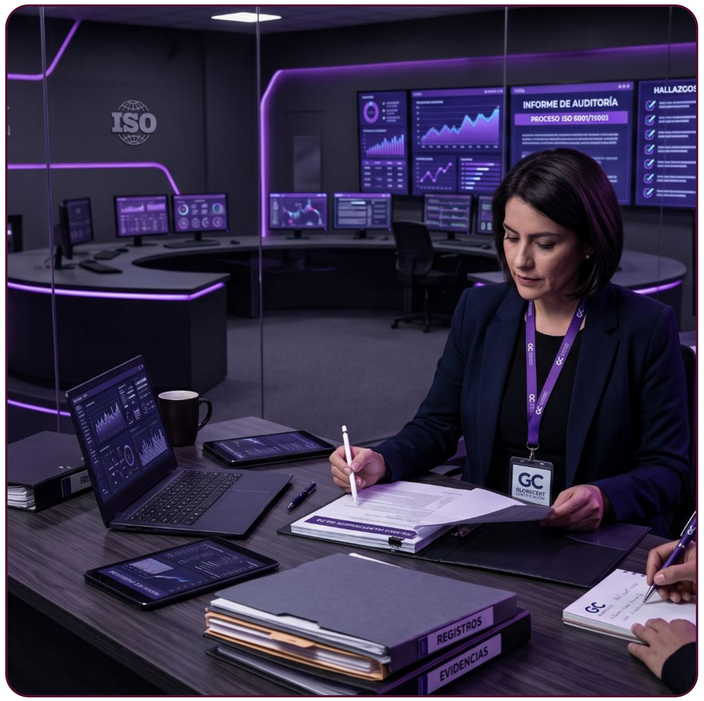
9. Requisitos relativos a los procesos

9.9 Registros relativos a solicitantes y clientes

Define los requisitos para mantener registros de auditorías y certificaciones, asegurando confidencialidad y trazabilidad.

El organismo de certificación debe aplicar los requisitos especificados en la Norma ISO/IEC 17021-1:2015, cláusula 9.9.

💡 Recuerda, Si una cláusula se ejecuta de manera idéntica y estándar, el documento lo declara directamente en su cuerpo principal (indicando que aplican los requisitos de la ISO/IEC 17021-1:2015) y se omite por completo de cualquier anexo de análisis para evitar engrosar el texto de forma redundante.



10. Requisitos del sistema de gestión para los organismos de certificación

Esta sección establece las opciones estructurales que tiene un organismo de certificación (OC) para implementar, mantener y demostrar que cuenta con un sistema de gestión que respalde la ejecución consistente y confiable de auditorías de SGSI (Sistemas de Gestión de la Seguridad de la Información). Su propósito central es asegurar que el propio ente que certifica opere bajo un marco de control institucionalizado, mitigando sus propios riesgos de operación y cumplimiento.

Estructura de la Cláusula 10: Dos opciones de cumplimiento

Opción A

Subcláusula 10.2

Si el organismo **no cuenta con ISO 9001**, debe estructurar y documentar requisitos mínimos de gestión internos.

Opción B

Subcláusula 10.3

Utilizando su certificación **ISO 9001 vigente**, el organismo debe proteger específicamente los requisitos técnicos y de imparcialidad.

10. Requisitos del sistema de gestión para los organismos de certificación

10.1 Opciones

El organismo de certificación debe establecer y mantener un sistema de gestión que sea capaz de apoyar y demostrar el logro coherente de los requisitos de este documento. Además de cumplir con los requisitos de las Cláusulas 5 a 9, el organismo de certificación debe implementar un sistema de gestión de acuerdo con:

- **10.1 Generalidades (General):** El organismo de certificación debe aplicar los requisitos especificados en la Norma ISO/IEC 17021-1:2015, Cláusula 10.

💡 Recuerda, Si una cláusula se ejecuta de manera idéntica y estándar, el documento lo declara directamente en su cuerpo principal (indicando que aplican los requisitos de la ISO/IEC 17021-1:2015) y se omite por completo de cualquier anexo de análisis para evitar engrosar el texto de forma redundante.

Gracias por su atención

🌐 www.valfraitconsulting.com