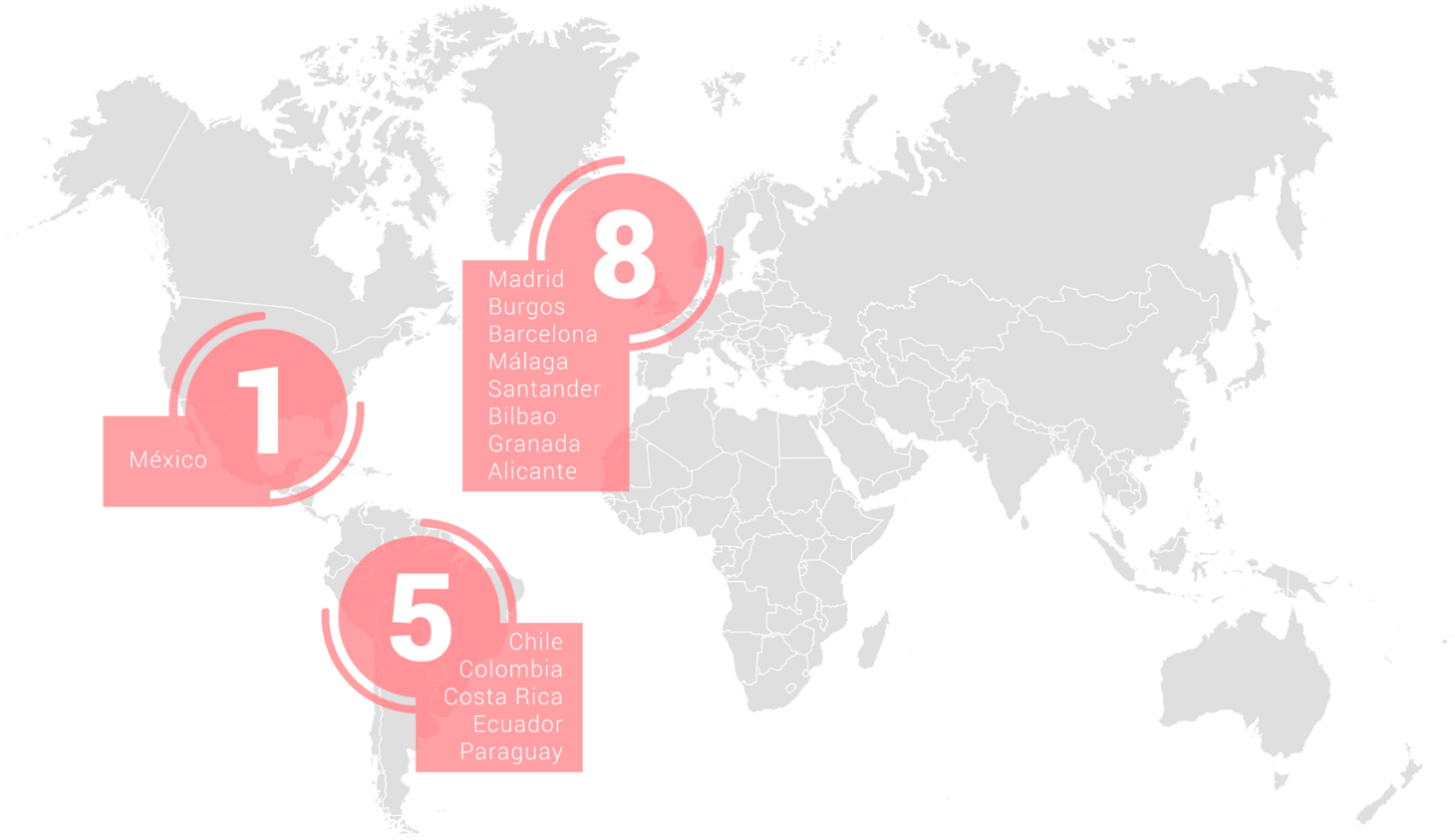
GrupoACMS
CONSULTORES

# GRUPO ACMS Consultores

ISO 27001 Seguridad de la Información




AENOR
ER
Empresa Registrada
ISO 9001

**(ER-0772/2013)**

**Alcance ISO 9001**

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

**Alcance ISO 27001**

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

**(SI-0021/2020)**

## ISO 27001 en Chile: te dejamos el sistema andando y te acompañamos hasta el certificado

Usted obtiene el Sistema de Gestión de Seguridad de la Información (SGSI) implantado y funcionando según ISO/IEC 27001:2022, con los riesgos evaluados, la Declaración de Aplicabilidad armada, la documentación lista y un consultor al lado tuyo hasta la auditoría de certificación. Y algo que casi nadie se va a ofrecer en Chile: le dejamos el sistema cargado en nuestro propio software ISO 27001, desarrollado por nosotros mismos, para que mantenerlo después no se le transforme en una pega de planillas Excel.

En simple: no le entregamos una carpeta con políticas. Le dejamos un sistema que funciona, que su equipo entiende y que resiste una auditoría.

## Nuestro software ISO 27001: el diferencial que sí se nota

Partamos por lo que nos distingue, porque es honesto ponerlo adelante.

La mayoría de las empresas no fracasa implantando la ISO 27001. Fracasa manteniéndola. Pasa el primer año, se va la persona que llevaba las planillas, llega la auditoría de seguimiento y nadie encuentra los registros de revisión de accesos, ni las actas del comité, ni la evidencia de que esa no conformidad se cerró.

Por eso desarrollamos ISOAPPWEB, nuestra propia plataforma para sistemas de gestión, con módulo específico para ISO 27001. No es un software de terceros que revendemos: lo desarrollamos nosotros, lo mantenemos nosotros y lo ajustamos a lo que necesitan nuestros clientes.

Qué le resuelve en concreto:

- Inventario de activos de información vivo y actualizado, no una planilla que quedó congelada el día de la auditoría.

- Riesgos y Declaración de Aplicabilidad enlazados: cambias un riesgo y ves de inmediato qué control te toca.

- Control documental de verdad. Se acabaron las tres versiones de la misma política dando vueltas en carpetas compartidas.

- Evidencias trazables, que es exactamente lo que te van a pedir demostrar en la auditoría.

- No conformidades, acciones correctivas, incidentes, capacitaciones, objetivos e indicadores en un solo lugar y con responsable y plazo asignado.

- Acceso web desde cualquier parte y dispositivo, con perfiles de usuario. Útil si tienes sucursales o equipos repartidos.

- Menos horas de su gente administrando el sistema. Menos horas es menos plata.

- Soporte directo de quien lo hizo. Si necesitas un ajuste, hablas con nosotros.

La diferencia de fondo es simple: quien diseña su sistema de gestión es el mismo que desarrolla el software donde lo vas a mantener. Están pensados juntos.

¿Quieres verlo funcionando? Pídanos una demostración sin compromiso.

Ojo: el uso del software es opcional. Si su empresa ya tiene una herramienta, nos adaptamos a la suya sin problema.

## ¿Qué es la ISO 27001 y qué le pide realmente?

ISO/IEC 27001 es la norma internacional certificable para sistemas de gestión de seguridad de la información. Te pide, en resumen, cinco cosas:

- Definir un alcance. Qué parte de su empresa, qué servicios, qué sedes y qué sistemas quedan dentro del certificado.

- Saber qué información tienes y dónde está. Activos de información, dueños, clasificación.

- Evaluar y tratar los riesgos con una metodología propia, documentada y repetible.

- Aplicar controles proporcionales a esos riesgos, y justificar por escrito cuáles aplicas y cuáles no. Ese documento se llama Declaración de Aplicabilidad (SoA) y es obligatorio.

- Medir, auditar internamente, revisar con la dirección y mejorar. El sistema tiene que estar vivo, no guardado.

Los requisitos certificables están en los capítulos 4 al 10 de la norma. El Anexo A entrega el catálogo de referencia de 93 controles, agrupados en cuatro temas: organizacionales, de personas, físicos y tecnológicos. La ISO/IEC 27002 es la guía que explica cómo implementar cada uno de esos controles, pero la 27002 no se certifica: la que se certifica es la 27001.

Y algo que conviene sacar del camino altiro: la ISO 27001 no le obliga a comprar tecnología. No exige un firewall de marca X ni un SIEM. Exige que usted demuestre que identificó sus riesgos y que aplicó controles razonables para ellos. La mayoría de las empresas descubre que ya tenía la mitad hecha, solo que sin orden ni evidencia.

## ¿Quién te está pidiendo la ISO 27001 en Chile?

En corto, y sin repetir lo que ya explicamos en detalle en nuestra página de seguridad de la información en Chile:

- Sus clientes corporativos. Banca, retail, telecomunicaciones y minería tienen programas formales de homologación de proveedores. Si les vendes software, servicios TI o procesamiento de datos, te van a pedir acreditar cómo proteges la información antes de firmar.

- Las licitaciones, públicas y privadas, donde el certificado funciona como criterio de solvencia técnica.

- La regulación. Si la ANCI le calificó como Operador de Importancia Vital bajo la Ley 21.663, una de sus obligaciones reforzadas es implementar un sistema de gestión de seguridad de la información. La norma no es obligatoria por ley, pero ISO 27001 es el estándar de referencia internacional para demostrar que ese sistema existe y funciona. El primer proceso de calificación de OIV sigue en curso: la nómina de la primera etapa se publicó a fines de 2025 y la segunda etapa, que

suma sectores como transporte, servicios sanitarios, combustibles y salud, quedó con nómina preliminar en abril de 2026 y su resumen de consulta pública se publicó en junio de 2026.

- La Ley 21.719 de protección de datos personales, que entra en plena vigencia el 1 de diciembre de 2026. No te exige certificarte, pero sí te exige demostrar medidas de seguridad. Un SGSI certificado es la forma más ordenada de tener esa evidencia lista.

En simple: la ley le dice qué cumplir. La ISO 27001 le da el cómo, ordenado, auditable y reconocido afuera.

## La Ley de Protección de Datos en Chile y la ISO 27001: la dupla que te protege

### ¿Qué gana su empresa con la certificación ISO 27001?

Implementar ISO 27001 no es un gasto de TI. Es una decisión estratégica que se paga sola. Estos son los beneficios concretos:

- Protección legal real frente a la Agencia de Protección de Datos Con evidencia documentada, reduces drásticamente su exposición a multas de hasta 5.000 UTM ? más de $350 millones de pesos.

- Ventaja competitiva en licitaciones y contratos Cada vez más empresas grandes, el Estado y los organismos internacionales exigen ISO 27001 como requisito para hacer negocios. Con el certificado, entras donde otros quedan afuera.

- Mayor confianza de sus clientes Una empresa que cuida los datos genera fidelidad. Y en Chile, eso se nota en el mercado. Los clientes prefieren a quien puede demostrar que su información está segura.

- Procesos ordenados y auditables Cada flujo de datos queda documentado, controlado y trazable. Se acabó la informalidad que te puede costar caro.

- Adaptación continua ante cambios legales o tecnológicos La norma exige mejora continua. Eso significa que su sistema siempre está al día, sin importar cómo evolucione la ley o la tecnología.

- Apertura a mercados internacionales ISO 27001 es el pasaporte para trabajar con empresas multinacionales y cumplir estándares internacionales como el RGPD europeo.

## Cómo es el proyecto, paso a paso

Sin letra chica y sin sorpresas a mitad de camino.

- Diagnóstico inicial . Revisamos cómo estás hoy: qué información manejas, qué controles ya tienes, qué proveedores críticos, qué te exigen sus contratos. Te decimos con claridad qué te falta y cuánto trabajo real hay por delante.

- Definición del alcance. Acá es donde más plata se pierde o se ahorra. Un alcance inflado te encarece el proyecto y la auditoría; uno mal recortado te entrega un certificado que su cliente no acepta. Lo definimos contigo, mirando quién te lo está pidiendo y para qué.

- Inventario de activos y apreciación de riesgos. Metodología aplicada a su realidad, no una plantilla de otra empresa. De acá sale el plan de tratamiento y la Declaración de Aplicabilidad.

- Diseño e implantación. Políticas, procedimientos y controles proporcionales a su tamaño y a su rubro. Documentación que su equipo entiende y usa, no manuales densos que nadie abre.

- Capacitación. Porque la mayoría de los incidentes entra por una persona, no por un firewall. Formamos a su gente para que el sistema lo sostengan ellos y no dependa de la consultora para siempre.

- Carga en el software. Dejamos el sistema montado en la plataforma antes de la auditoría, no después.

- Auditoría interna y revisión por la dirección. Encontramos y corregimos los hallazgos antes de que los vea el certificador. Este paso es el que marca la diferencia entre llegar tranquilo o llegar a apagar incendios.

- Acompañamiento en la certificación. La auditoría de certificación tiene dos etapas: una revisión documental (Etapa 1) y una auditoría en terreno de la implementación (Etapa 2). Te acompañamos en las dos y en el cierre de las no conformidades si aparecen.

- Mantenimiento. El certificado tiene un ciclo de tres años, con auditorías de seguimiento anuales y una recertificación al final del ciclo. Seguimos contigo en todas.

## ¿Cuánto demora y de qué depende el precio?

No le vamos a tirar una cifra de folleto, porque sería mentirle. Lo que sí podemos decirle es qué mueve la aguja:

- El alcance. Una unidad de negocio no cuesta lo mismo que toda la empresa con cinco sedes.

- La cantidad de sedes y de personas dentro del alcance.

- La complejidad de sus sistemas y cuánta infraestructura externalizas (nube, proveedores TI, datacenter).

- Su punto de partida. No es lo mismo llegar con cero que llegar con ISO 9001 ya andando.

- Cuánto se compromete su equipo interno. Este es el factor que más acelera o frena un proyecto, y no depende de nosotros.

Recuerde además que la consultoría y la certificación son dos costos distintos: nosotros le implantamos el sistema, y el organismo certificador acreditado te cobra aparte la auditoría. Se lo transparentamos desde la propuesta para que arme bien su presupuesto.

En el diagnóstico inicial le entregamos un plazo estimado y una propuesta con presupuesto cerrado para su caso concreto.

## Los cinco errores que hacen fracasar una certificación ISO 27001

Los vemos siempre, y todos se pueden evitar:

- Definir mal el alcance. Poner "toda la organización" porque suena mejor, y después no poder sostenerlo en la auditoría.

- Copiar la Declaración de Aplicabilidad. Poner los 93 controles del Anexo A con una columna de "sí/no" y sin trazarlos a un riesgo real. Es lo primero que un auditor con experiencia va a picar.

- Tratarlo como un proyecto del área de TI. La ISO 27001 toca RR.HH., legal, compras, operaciones y dirección. Si es solo de TI, no se sostiene.

- Olvidarse de los proveedores. Los controles sobre terceros son de los que más no conformidades generan: contratos sin cláusulas de seguridad, accesos que quedaron abiertos, servicios en la nube sin evaluar.

- No tener dónde guardar la evidencia. Este es el clásico. El sistema se implanta bien y se muere en el año dos por pura falta de herramienta. Justamente para eso está nuestro software.

## Intégrela con lo que ya tiene

ISO 27001 comparte la misma estructura de alto nivel que ISO 9001, ISO 14001 e ISO 45001.

Si ya está certificado en calidad, medio ambiente o prevención de riesgos laborales, sumar seguridad de la información te sale más rápido y más barato: un solo análisis de contexto, una sola gestión documental, una sola auditoría interna y, habitualmente, auditorías de certificación combinadas.

¿Y si necesitas más de una norma de seguridad? En nuestra página de seguridad de la información en Chile le explicamos cuándo conviene sumar ISO 20000-1 (servicios TI), ISO 22301 (continuidad del negocio), ISO 27701 (privacidad) o ISO 42001 (inteligencia artificial).

## ¿Por qué elegir a Grupo ACMS Consultores para su certificación ISO 27001 en Chile?

Si necesita asesoramiento consúltenos sin compromiso. Rellene el formulario de contacto y nos pondremos en contacto con su organización.

Compromisos y garantías de Grupo ACMS Consultores

Aspecto

Ventaja líder

Experiencia

Más de 25 años de trayectoria en consultoría y formación. Fundado en 1998, con más de 1.000 proyectos implantados con éxito.

Certificados propios

Disponemos de los certificados ISO 9001 e ISO 27001 en ACMS España.

Porfolio y diversificación

Amplia gama de servicios de consultoría en certificación (ISO 9001, ISO 14001, ISO 45001, etc.) y acreditación (ISO 15189, ISO 17025, ISO 17020, entre otras). Capacidad para abordar proyectos integrados y multisectoriales.

Precio

Presupuestos personalizados con condiciones de pago adaptadas a las necesidades de cada cliente.

Garantía

Compromiso de acompañamiento hasta la certificación o acreditación, asegurando resultados tangibles.

Desarrollo y soporte

Asesoramiento continuo durante todo el proceso de implantación, desde el diagnóstico inicial hasta la auditoría final.

Desarrollo de sistemas de gestión totalmente adaptados a cada organización evitando la burocracia.

Diseño de procedimientos documentados, flujogramas y cuadros de gestión de procesos de fácil comprensión, sustituyendo manuales densos, para facilitar la toma de decisiones.

Referencias

El GRUPO ACMS trabaja con pequeñas y grandes empresas tanto del sector público como privado.

Oficinas

Presencia nacional e internacional con sedes en Chile, España y México, lo que permite cercanía y atención personalizada.

Software propio

Plataforma ISOAPPWEB desarrollada internamente para el mantenimiento y control de la norma ISO 27001 que agiliza procesos, reduce costes y facilita el control documental.

Plataforma formación

Campus online con cursos especializados en diversas áreas donde ofrecemos asesoramiento. Incluye programas actualizados y accesibles en modalidad e-learning.

Grupo ACMS Consultores Chile Consultora especializada en diseño, implantación y mantenimiento de Sistemas de gestión

## Preguntas frecuentes sobre ISO 27001 en Chile

¿Ustedes certifican la ISO 27001?

No. Somos consultores: implantamos el sistema y lo dejamos preparado para la auditoría. El certificado lo emite un organismo certificador independiente y acreditado, tal como exigen las reglas de imparcialidad. Te orientamos para que elijas el más adecuado a su caso.

¿Cuál es la versión vigente de la ISO 27001?

La ISO/IEC 27001:2022, publicada en octubre de 2022. Los certificados bajo la versión 2013 dejaron de ser válidos el 31 de octubre de 2025. No existe una versión 2026 de la norma.

Me quedé con el certificado en la versión 2013 y se me venció el plazo. ¿Qué hago?

Hay que certificar de nuevo sobre la versión 2022. La buena noticia es que buena parte de su sistema sirve: normalmente hay que actualizar la Declaración de Aplicabilidad al nuevo Anexo A, revisar la apreciación de riesgos y cerrar las brechas de los controles nuevos. En el diagnóstico te decimos exactamente cuánto es rescatable.

¿Cuántos controles tiene la ISO 27001:2022?

El Anexo A contiene 93 controles de referencia, agrupados en cuatro temas: organizacionales, de personas, físicos y tecnológicos. No todos te aplican: la Declaración de Aplicabilidad es justamente el documento donde justificas cuáles sí y cuáles no, en función de sus riesgos.

¿Qué es la Declaración de Aplicabilidad?

Es el documento obligatorio donde declaras qué controles del Anexo A aplicas, cómo los aplicas y por qué excluyes los que excluyes. Es lo primero que revisa un auditor y una de las principales fuentes de no conformidades cuando está copiada de una plantilla.

¿Cuánto se demora certificarse en ISO 27001 en Chile?

Depende del alcance, del tamaño de la organización, de la complejidad de sus sistemas y de cuánto se comprometa su equipo. En el diagnóstico inicial te entregamos un plazo estimado para su caso, no una cifra genérica.

¿La ISO 27001 es obligatoria en Chile?

No. Las certificaciones ISO son voluntarias. Lo obligatorio es cumplir la ley: la Ley 21.663 de ciberseguridad si prestas un servicio esencial o te calificaron como OIV, y la Ley 21.719 de datos personales desde el 1 de diciembre de 2026. La ISO 27001 no es la obligación, pero sí es la forma más reconocida de demostrar que la cumples.

¿Sirve para una empresa que no es de tecnología?

Sí. Información maneja todo el mundo: una clínica con fichas de pacientes, un municipio, una corredora, una constructora con planos y contratos, un retail con datos de clientes. La norma es genérica y se ajusta al tamaño y al rubro.

¿El software está incluido en el servicio?

Se lo presentamos dentro del proyecto de implantación y las condiciones quedan indicadas en la propuesta. La idea es que el sistema quede cargado y funcionando antes de la auditoría. Su uso es opcional: si su empresa ya tiene una herramienta, trabajamos con la tuya.

¿Qué pasa después de obtener el certificado?

El certificado tiene un ciclo de tres años, con auditorías de seguimiento anuales y una recertificación al cierre del ciclo. Le acompañamos en todas para que la renovación no se te transforme en un problema. Para eso mismo sirve el software.

## Solicite su diagnóstico ISO 27001

Cuéntenos si parte de cero, si se quedó en la versión 2013 o si le están pidiendo el certificado para un cliente o una licitación, y un consultor de Grupo ACMS Chile se pondrá en contacto con su empresa.

Grupo ACMS Chile ? Av. Pdte. Kennedy 7440, Oficina 701, Región Metropolitana ? WhatsApp: (+56) 9 8149 5541

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

## Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

## Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

## Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

## CDMX

José González Varela 15 14700 Tlalpan (Ciudad de México)

Tfno.: (+52) 5514 10 12 07

## Chile

Av. Pdte. Kennedy 7440, Of. 701 7630000 Vitacura, Área Metropolitana - Santiago. Regiones de Valparaíso, Metropolitana (Santiago) y O´higgins

Tfno.: WhatsApp (+56) 981495541 y (+56) 994713521

## Veracruz

Avda 21 esquina calle 44 No.4402 Nuevo Elizabeth Córdoba

Tfno.: (+52) 55 6576 8293

## Nuevo León

Angelo 125, Frac. Privadas de San Miguel 67130 Guadalupe - Noreste de México - Estado: Nuevo León

Tfno.: (+52) 5565768293

## Aguascalientes

Calle Livorno, 534 Aguascalientes Queretaro - Guanajuato ? Aguascalientes

Tfno.: (+52) 449 386 8693

www.grupoacms.com

informacion@grupoacms.com