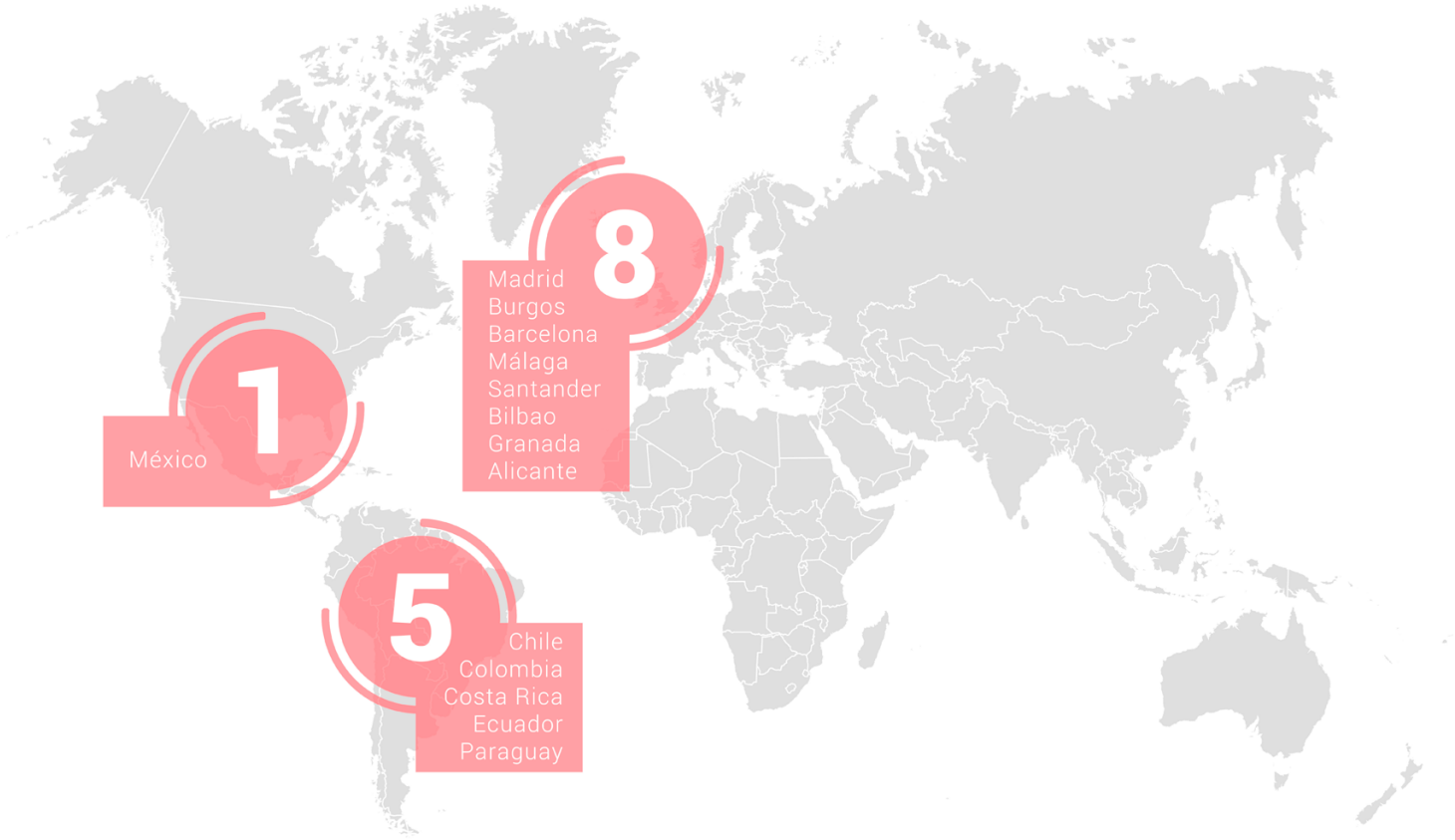
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Seguridad de la Información en Chile - Consultoría SGSI



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)

Publicado el 22/07/2026 - Actualizado el 21/09/2026

Seguridad de la información en Chile: lo acompañamos hasta el certificado

Usted obtiene un sistema de gestión de seguridad de la información funcionando de verdad en su empresa ?no una carpeta de políticas que nadie abre?, un consultor a su lado durante todo el proceso y el respaldo hasta la auditoría de certificación.

En la práctica eso significa saber qué información tiene, dónde está y quién la toca; controles que su gente aplica; evidencias listas para mostrar; y el certificado en la mano para licitaciones, para mandantes y para clientes corporativos que hoy se lo están pidiendo antes de firmar.

Y algo que nos diferencia: le damos acceso además a nuestro propio software para gestionar el sistema, desarrollado por nosotros, para que mantenerlo no se le transforme en una pega eterna de planillas Excel.

Por qué en Chile esto se puso serio

Hasta hace poco, la seguridad de la información en Chile era un tema del área de TI. Hoy es un tema de directorio, y por tres razones concretas.

Uno: Chile ya tiene ley de ciberseguridad. La Ley 21.663, Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información, se publicó el 8 de abril de 2024 y creó la Agencia Nacional de Ciberseguridad (ANCI).

Si su empresa presta un servicio esencial ?energía, combustibles, agua, telecomunicaciones, infraestructura digital, servicios TI gestionados a terceros, transporte, banca y medios de pago, seguridad social, servicios postales, salud, farmacéutico? tiene deberes exigibles: gestionar los riesgos de sus redes y sistemas de forma continua, tener capacidad real de detectar y responder incidentes, y reportarlos al CSIRT Nacional dentro de plazos cortos, empezando por una alerta temprana en las primeras horas.

Y si la ANCI lo califica como Operador de Importancia Vital, la exigencia sube: ahí ya se le pide implementar un sistema de gestión de seguridad de la información, planes de continuidad operacional y de ciberseguridad, auditorías y simulacros periódicos, y un delegado de ciberseguridad.

Las multas escalan por tramos y en las infracciones más graves llegan a 40.000 UTM.

Dos: el 1 de diciembre de 2026 entra en vigencia la nueva ley de datos personales. La Ley 21.719, publicada en diciembre de 2024, reemplaza el esquema de la Ley 19.628 ?que llevaba más de dos décadas prácticamente sin dientes? y crea la Agencia de Protección de Datos Personales, con facultades para fiscalizar y sancionar.

Trae registro de actividades de tratamiento, notificación obligatoria de brechas, derechos reforzados de los titulares, la figura del Delegado de Protección de Datos y multas de hasta 20.000 UTM que, en los casos más graves y con reincidencia, pueden escalar a un porcentaje de los ingresos anuales de la empresa. Es un modelo muy parecido al europeo.

Si usted trata datos de personas ?o sea, casi cualquier empresa? esto le aplica.

Tres: se lo va a pedir el mercado antes que la autoridad. Las licitaciones públicas y las homologaciones de proveedores de empresas grandes ya incorporan requisitos de seguridad de la información. Y si usted le vende servicios TI, software o procesamiento de datos a una empresa regulada, el riesgo de ella pasa a ser su requisito: le van a exigir acreditar cómo protege la información antes de firmar el contrato.

En simple: la ley le dice qué tiene que cumplir. Las normas ISO le dan el cómo, ordenado, auditable y reconocido afuera.

Y ojo con algo importante: la Ley 21.663 no le obliga a certificarse en ninguna norma en particular, pero ISO 27001 es el estándar internacional de referencia para acreditar que usted tiene un sistema de gestión de seguridad de la información andando. Es el camino más corto y más reconocido para demostrarlo.

Qué incluye nuestro servicio de seguridad de la información en Chile

- Diagnóstico inicial. Revisamos cómo está hoy su organización ?activos de información, controles, proveedores, contratos, incidentes previos, obligaciones legales que le aplican? y le decimos con claridad qué le falta para cumplir y para certificar. Sin letra chica.

- Definición del alcance. Uno de los puntos donde más plata se pierde. Un alcance mal definido le encarece el proyecto y la auditoría; uno bien definido le da el certificado que su cliente realmente necesita ver.

- Análisis y tratamiento de riesgos. Metodología aplicada a su realidad, no una plantilla de otra empresa. De ahí sale la declaración de aplicabilidad y el plan de trabajo.

- Diseño e implantación del sistema. Políticas, procedimientos y controles proporcionales a su tamaño y a su rubro. Documentación que su equipo entiende y usa.

- Requisitos legales aplicables. Identificados y trazados: Ley 21.663 si le corresponde, Ley 21.719, normativa sectorial de su industria y los compromisos contractuales con sus clientes.

- Capacitación del personal. Porque la mayoría de los incidentes entra por una persona, no por un firewall. Formación presencial u online para que el sistema lo sostenga su equipo y no dependa de la consultora.

- Auditoría interna y revisión por la dirección. Detectamos y corregimos los hallazgos antes de que los vea el organismo certificador.

- Software propio. Le dejamos el sistema cargado en nuestra plataforma para que el mantenimiento sea rápido y ordenado.

- Acompañamiento en la auditoría de certificación y en el cierre de las no conformidades, si las hubiera.

- Mantenimiento posterior. Lo apoyamos en las auditorías de seguimiento y en la renovación del certificado.

Las normas que implantamos en Chile

ISO/IEC 27001 ? Seguridad de la información

La norma base y la más pedida. Define los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI): identificar sus activos de información, evaluar los riesgos, aplicar controles y mejorar de forma continua.

Aplica a cualquier tamaño y rubro. Es la que le abren la puerta en licitaciones y homologaciones, y la referencia natural cuando la ANCI o un cliente grande le pide acreditar su gestión de seguridad. La versión certificable vigente es ISO/IEC 27001:2022.

Ver ISO 27001 en Chile

ISO/IEC 20000-1 ? Gestión de servicios TI

Si usted presta servicios de tecnología ?soporte, mesa de ayuda, cloud, desarrollo, servicios gestionados?, esta es la norma que ordena cómo los entrega: niveles de servicio comprometidos y medidos, gestión de incidencias, cambios y capacidad. Se lleva muy bien con ISO 27001: una dice cómo protege la información, la otra cómo entrega el servicio. Juntas son el combo que piden los clientes corporativos a sus proveedores TI.

ISO 22301 ? Continuidad del negocio

Responde a una pregunta incómoda: si mañana su operación se cae ?por un ciberataque, por un corte, por un evento natural?, ¿en cuánto tiempo vuelve, y quién decide qué? ISO 22301 estructura el análisis de impacto en el negocio, las estrategias de recuperación y los planes de continuidad, con ejercicios que se prueban de verdad. En un país sísmico y con una regulación que ya exige continuidad operacional a los operadores más críticos, esta norma dejó de ser un lujo.

ISO/IEC 27701 ? Privacidad y datos personales

El sistema de gestión de privacidad. Es la pieza que conecta directamente con la Ley 21.719: registro de tratamientos, roles de responsable y encargado, derechos de los titulares, gestión de brechas.

La versión publicada en octubre de 2025 trae un cambio importante: ahora puede implantarse y certificarse de forma independiente, sin necesidad de tener antes ISO 27001, aunque lo habitual y lo más eficiente sigue siendo trabajarlas juntas.

ISO/IEC 42001 ? Gestión de la inteligencia artificial

La primera norma internacional certificable para gobernar el uso de la IA en una organización: quién autoriza qué uso, con qué evaluación de riesgos, con qué supervisión humana y con qué trazabilidad. Sirve tanto si usted desarrolla IA como si simplemente la usa en procesos que afectan a personas o a decisiones del negocio.

Hoy es un diferenciador comercial fuerte; todo indica que en pocos años se lo van a pedir igual que hoy le piden ISO 27001.

¿Y cuál me sirve a mí?

Es la pregunta que más nos hacen. Una guía rápida, sin compromiso:

- "Me la están pidiendo para vender o para una licitación." ? ISO 27001.

- "Presto servicios TI a otras empresas." ? ISO 27001 + ISO 20000.

- "Manejo muchos datos de personas y me preocupa diciembre de 2026." ? ISO 27001 + ISO 27701.

- "Si mi operación se cae, se cae el negocio de mi cliente." ? ISO 27001 + ISO 22301.

- "Estamos metiendo IA en procesos importantes." ? ISO 42001.

- "Creo que soy servicio esencial o me van a calificar como OIV." ? conversemos primero; ahí el diagnóstico manda.

En el diagnóstico inicial le decimos cuál corresponde en su caso y en qué orden, sin venderle normas que no necesita.

Nuestro diferencial: software propio

Acá está la diferencia grande, y es honesto decirlo: la mayoría de las empresas no fracasa implantando el sistema, fracasa manteniéndolo. 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.

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 adaptamos a lo que necesitan nuestros clientes.

Qué gana usted con eso:

- Control documental de verdad. Se acabaron las versiones sueltas en carpetas compartidas y el "¿cuál era la política vigente?".

- Evidencias trazables, que es justo lo que le van a pedir demostrar en una auditoría o en una fiscalización.

- Todo en un solo lugar: inventario de activos, riesgos, declaración de aplicabilidad, no conformidades, acciones correctivas, capacitaciones, incidentes, hallazgos de auditoría y seguimiento de objetivos.

- Acceso desde cualquier parte, útil si tiene sucursales o equipos distribuidos.

- Menos horas de su gente administrando el sistema, y por lo tanto menos costo real.

- Soporte directo de quien lo hizo. Si necesita un ajuste, habla con nosotros.

Se integra con lo que ya tiene

Todas estas normas comparten la misma estructura de alto nivel que ISO 9001, ISO 14001 e ISO 45001. Si usted ya está certificado en calidad, medio ambiente o prevención de riesgos laborales, sumar seguridad de la información le sale más rápido, más barato y con menos papeleo, porque se monta sobre lo que ya tiene funcionando: un solo contexto, una sola gestión de riesgos, una sola auditoría interna y, habitualmente, auditorías de certificación combinadas. Eso se llama sistema integrado de gestión y es como trabajamos habitualmente.

Cómo trabajamos

- Contacto y diagnóstico. Entendemos su actividad, su alcance, sus sistemas y sus plazos.

- Propuesta y planificación. Presupuesto cerrado y calendario acordado. Sin sorpresas a mitad de camino.

- Implantación. Trabajo conjunto con su equipo, con seguimiento periódico y con la plataforma andando desde el principio.

- Auditoría interna. Verificamos que el sistema funciona y corregimos lo que falte.

- Certificación. Lo acompañamos ante el organismo certificador acreditado que usted elija.

- Mantenimiento. Seguimos con usted en las auditorías de seguimiento y en la renovación.

Por qué elegir a Grupo ACMS en Chile

Compromisos y garantías de nuestro servicio

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, ISO 27001, ISO 20000, ISO 22301, ISO 22301, ISO 27701, ISO 42001 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 asegurando resultados tangibles.

Desarrollo y soporte

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

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

¿Es obligatorio certificarse en alguna de estas normas en Chile?

No. Las certificaciones ISO son voluntarias. Lo obligatorio es cumplir la ley: la Ley 21.663 si usted presta un servicio esencial, y la Ley 21.719 en materia de datos personales desde el 1 de diciembre de 2026. Ahora bien, implantar la norma es la forma ordenada y demostrable de cumplir, y además le sirve comercialmente. Las dos cosas con un solo esfuerzo.

¿Por dónde empiezo si no tengo nada?

Por el diagnóstico. En una reunión y una revisión de su realidad podemos decirle qué norma le corresponde, qué alcance conviene y cuánto trabajo real hay por delante. No cobramos por decirle eso.

¿Ustedes certifican?

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

¿Puedo implantar varias normas a la vez?

Sí, y suele ser lo más conveniente. Comparten estructura, contexto, gestión de riesgos, auditoría interna y buena parte de la documentación. Hacerlas por separado le cuesta más caro y le duplica el papeleo.

¿Cuánto se demora?

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

¿Esto sirve solo para empresas de tecnología?

No. Información maneja todo el mundo: una clínica, un municipio, una empresa de servicios financieros, una constructora con planos y contratos, un retail con datos de clientes. La norma es genérica y se adapta al tamaño y al rubro.

¿El software está incluido en el servicio?

Le presentamos la plataforma dentro del proyecto de implantación y le indicamos las condiciones en la propuesta. La idea es que el sistema quede cargado y funcionando antes de la auditoría, no después. De todas formas es opcional el uso del software. Su empresa ya puede tener uno y en ese caso nos adaptaríamos al suyo.

¿Qué pasa después de obtener el certificado?

El sistema tiene que mantenerse vivo y se somete a auditorías de seguimiento del organismo certificador. Lo acompañamos en esa etapa para que la renovación no se le transforme en un problema, y para eso mismo sirve el software.

Solicite su diagnóstico de seguridad de la información

Cuéntenos cómo está hoy su empresa y un consultor de Grupo ACMS Chile se pone en contacto con usted.

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.: (+56) 981495541. Whatsapp (+56) 9 9471 3521

Aguascalientes

Calle Livorno, 534 Aguascalientes Queretaro - Guanajuato ? Aguascalientes

Tfno.: (+52) 449 386 8693

www.grupoacms.com

informacion@grupoacms.com