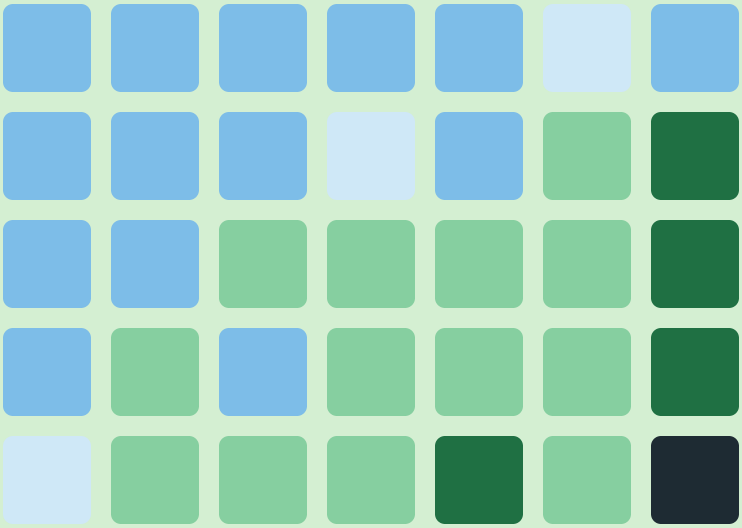
ATTESTA
CONSULTORA

GUÍA 02 · SEGURIDAD DE LA INFORMACIÓN

ISO/IEC 27001:2022 en 6 meses, mes a mes

Qué es un sistema de gestión de seguridad de la información, qué hace su organización y qué hace la consultora en cada etapa, y qué ocurre después, frente al organismo certificador.



attesta.cl · contacto@attesta.cl

Octubre 2026

EN RESUMEN

- ISO/IEC 27001:2022 es la norma internacional que define cómo gestionar la seguridad de la información de forma sistemática y verificable. Se puede certificar.
- En seis meses es posible diseñar el sistema, ponerlo en operación con evidencia y cerrar el primer ciclo de auditoría interna y revisión por la dirección, condición previa a la auditoría de certificación.
- El sistema lo implementa y lo opera su organización. La consultora aporta método, acompañamiento y revisión; el certificado lo otorga un organismo acreditado.

01

Qué es un sistema de gestión de seguridad de la información

Un sistema de gestión de seguridad de la información (SGSI) es el conjunto de políticas, responsabilidades, procesos y controles con que una organización identifica sus riesgos de seguridad, los trata y demuestra que lo hace de manera continua. La norma `ISO/IEC 27001:2022` establece sus requisitos en dos partes.

PARTE DE LA NORMA	CONTENIDO
Cláusulas 4 a 10	Requisitos del sistema de gestión: contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. Son obligatorios en su totalidad.
Anexo A	93 controles de referencia agrupados en cuatro temas: 37 organizacionales, 8 de personas, 14 físicos y 34 tecnológicos. Cada organización decide cuáles aplica según sus riesgos y lo justifica en la Declaración de Aplicabilidad.

La certificación no evalúa si la organización es invulnerable. Evalúa si gestiona sus riesgos de forma ordenada, si aplica los controles que declaró y si puede demostrarlo con registros.

02

Quién hace qué

RESPONSABLE	QUÉ LE CORRESPONDE
Su organización	Designar a un responsable del sistema con tiempo asignado, aprobar el alcance y las políticas, asignar recursos, implementar los controles y operar el sistema en el día a día.

RESPONSABLE	QUÉ LE CORRESPONDE
La consultora	Aportar el método y las plantillas, conducir el análisis de riesgos, revisar la documentación, acompañar la implementación de los controles, montar el tablero de evidencias y preparar a la organización para la auditoría de certificación.
El organismo certificador	Auditar el sistema y, si cumple, otorgar el certificado. Es una entidad acreditada e independiente de la consultora.

03

El programa, mes a mes

Mes 1 Alcance y contexto
Mes 2 Riesgos
Mes 3 Aplicabilidad y tratamiento
Mes 4 Políticas y controles
Mes 5 Operación con evidencia
Mes 6 Auditoría interna y revisión

Mes 1 · Alcance y contexto

Se realiza un diagnóstico inicial frente a la norma y se define qué parte de la organización cubre el sistema: procesos, sedes, sistemas y personas. Se identifican las partes interesadas y sus requisitos, se aprueba la política de seguridad de la información y se asignan los roles y responsabilidades.

Mes 2 · Evaluación de riesgos

Se adopta una metodología de riesgos, se levanta el inventario de activos de información dentro del alcance y se evalúa, para cada uno, qué amenazas lo afectan, qué tan probable es que ocurran y qué impacto tendrían. El resultado es un registro de riesgos priorizado.

Mes 3 · Declaración de Aplicabilidad y plan de tratamiento

Para cada riesgo se decide cómo tratarlo y con qué controles. Se elabora la Declaración de Aplicabilidad, que indica cuáles de los 93 controles del Anexo A se aplican, cuáles no y por qué. Se fijan los objetivos de seguridad y un plan de tratamiento con responsables y plazos.

Mes 4 · Políticas, procedimientos y controles

Se redactan y aprueban las políticas y los procedimientos necesarios, y se implementan los controles prioritarios: gestión de accesos, respaldos, gestión de proveedores, respuesta a incidentes y concientización del personal, entre otros. Cada control debe dejar un registro que demuestre que funciona.

Mes 5 · Operación con evidencia

El sistema opera y genera evidencia: registros de accesos, de incidentes, de revisiones de proveedores y de capacitación. Se definen los indicadores y se reúnen en un tablero que muestra el estado de cada control, su responsable y su evidencia.

Mes 6 · Auditoría interna y revisión por la dirección

Se realiza la auditoría interna, con la objetividad e imparcialidad que exige la cláusula 9.2 de la norma, y se registran las no conformidades y las acciones correctivas. La dirección revisa el desempeño del sistema y toma decisiones sobre su mejora. Con ese ciclo cerrado, la organización queda preparada para solicitar la auditoría de certificación.

> **POR QUÉ LOS SEIS MESES SON REALISTAS**
>
> El plazo depende del alcance, del tamaño de la organización y de su madurez inicial. Se cumple cuando el alcance es acotado, existe un responsable interno con tiempo asignado y la dirección aprueba a tiempo. Un alcance amplio o una organización sin prácticas previas de seguridad pueden requerir más tiempo; el diagnóstico inicial lo indica antes de comprometer fechas.

04

Después de los seis meses: la certificación

La certificación la otorga un organismo de certificación acreditado. El proceso tiene dos etapas.

1. **Etapa 1.** El organismo revisa la documentación del sistema y verifica que la organización está preparada para la auditoría principal.
2. **Etapa 2.** El organismo audita la implementación: comprueba con entrevistas y registros que los controles declarados funcionan.

Si el resultado es favorable, el certificado tiene una vigencia de tres años, con auditorías de seguimiento anuales y una auditoría de recertificación al término del ciclo. El costo del organismo certificador se paga aparte y directamente a él.

05

Lo que no prometemos

- **No certificamos.** Solo un organismo acreditado puede otorgar el certificado.
- **No garantizamos el certificado.** El resultado depende de que el sistema funcione y de la evaluación independiente del organismo. Lo que sí entregamos es un sistema preparado y la evidencia para demostrarlo.
- **No acortamos etapas.** Un sistema sin operación real y sin evidencia puede aprobar la revisión documental, pero difícilmente la auditoría de implementación.

SIGUIENTE PASO

¿Cuánto le falta a su organización para certificarse?

El Diagnóstico ISO/IEC 27001 mide su nivel de cumplimiento por cláusula y por control, y entrega una hoja de ruta a 90, 180 y 365 días. Es el punto de partida para fijar un plazo realista. Solicite una reunión de diagnóstico de 30 minutos.

attesta.cl/contacto

SOBRE ATTESTA

Attesta es una consultora de gestión y protección de datos y de seguridad de la información. Nuestro equipo acompaña a las organizaciones en la implementación de su sistema de gestión ISO/IEC 27001 y en su certificación, y deja la evidencia de cada control medida y a la vista.

attesta.cl · contacto@attesta.cl · Av. Manquehue Sur 520, Of. 205, Las Condes

Aviso. Esta guía es informativa. Los plazos indicados son referenciales y dependen del alcance y de la situación de cada organización.

FUENTES

- ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- ISO/IEC 17021-1. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.