

CURSO IMPLEMENTADOR EXPERTO ISO 27001 - SGSI: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Curso Certificado - Online Sincrónico



El programa desarrolla competencias profesionales en la **implementación, mantenimiento y mejora continua de los SGSI** conforme a estándares internacionales.

Adquirirá conocimientos prácticos sobre los **principios, metodologías y controles** necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información de su organización.

Alineado con las normas: **ISO/IEC 27001:2022**, **ISO/IEC 27002:2022** e **ISO/IEC 27005:2022**, así como a los lineamientos de la **Ley Marco de Ciberseguridad** de Chile (2024), asegurando un enfoque actualizado, normativo y aplicable a distintos contextos operativos.

NIVEL DEL CURSO

► **AVANZADO - INTENSIVO**

(Requiere nociones teóricas previas)

DURACIÓN DEL CURSO

► **15 HORAS TOTALES**

(Divididas en 2 días)

METODOLOGÍA

► **IMPLEMENTACIÓN - PRÁCTICA**

(Más de 50 recursos y ejemplos reales)

FECHA DE INCIO

► **MIÉRCOLES 14 Y JUEVES 15 - ENERO**

(9:00 a 13:00 – 14:00 a 17:30 Hrs) GMT-3

¿QUÉ APRENDERÁS EN EL CURSO? 12 UNIDADES:

(DÍA 1)

UNIDAD 1: Fundamentos y Diagnóstico Inicial del SGSI

- Principios y objetivos del SGSI.
- Estructura y propósito de la norma ISO/IEC 27001:2022.
- Integración con otros sistemas ISO (27701, 22301, 9001).
- Diagnóstico inicial y análisis GAP.
- Identificación de requisitos legales y contractuales.
- Relación con la Ley Marco de Ciberseguridad (Art. 8-13).
- Planificación del proyecto de implementación Alignment.

Material Entregable:

- Plantilla "Análisis GAP ISO 27001:2022".
- Checklist de requisitos y evidencias.
- Guía de estructura ISO 27001.
- Plantilla "Plan de Proyecto SGSI Alignment".
- Ejemplo: Diagnóstico de madurez inicial.

UNIDAD 2: Contexto Organizacional y Partes Interesadas

- Identificación del contexto interno y externo.
- Análisis PESTEL y FODA cibernético.
- Identificación de partes interesadas y sus expectativas.
- Determinación del alcance del SGSI.
- Evaluación de madurez organizacional.
- Elaboración del mapa de interdependencias de servicios críticos.

Material Entregable:

- Plantilla "Análisis de Contexto SGSI".
- Matriz PESTEL y FODA editable.
- Mapa de Partes Interesadas.
- Formato de Determinación de Alcance.
- Guía Alignment de madurez contextual.
- Procedimiento "Gobernanza y Gestión".

UNIDAD 3: Liderazgo, Gobernanza y Política de Seguridad

- Responsabilidad de la alta dirección en el SGSI.
- Política de Seguridad: estructura, aprobación y difusión.
- Comité de Seguridad y gobierno de la información.
- Roles y responsabilidades SGSI.
- Comunicación y cultura de seguridad. Gobernanza digital y responsabilidad ejecutiva.

Material Entregable:

- Plantilla editable de Política SGSI.
- Acta de creación del Comité de Seguridad.
- Matriz RACI de responsabilidades.
- Guía Alignment de liderazgo y gobernanza.
- Procedimiento "Gobernanza y Gestión".

UNIDAD 4: Planificación y Objetivos Estratégicos del SGSI

- Definición de objetivos de seguridad (SMART).
- Identificación de riesgos y oportunidades.
- KPI y KRI para medición de desempeño.
- Planificación de acciones preventivas y correctivas.
- Alineamiento con la estrategia institucional.
- Priorización de recursos y proyectos SGSI.

Material Entregable:

- Plantilla "Plan de Objetivos SGSI" (Excel).
- Matriz SMART de objetivos.
- Plantilla KPI/KRI SGSI.
- Procedimiento "Gobernanza y Gestión".
- Ejemplo Alignment de objetivos estratégicos.

UNIDAD 5: Identificación y Gestión de Riesgos

- Inventario de activos de información. Identificación de amenazas y vulnerabilidades.
- Evaluación de riesgos (probabilidad e impacto).
- Elaboración de matriz de riesgos y mapa de calor.
- Plan de tratamiento de riesgos y monitoreo.
- Alineamiento con la gestión de continuidad y Ley Marco.

Material Entregable:

- Plantilla "Matriz de Riesgos SGSI".
- Catálogo de amenazas y vulnerabilidades.
- Plantilla de Plan de Tratamiento de Riesgos.
- Procedimiento "Gestión de Riesgos".
- Ejemplo Alignment de riesgo cibernético crítico.

UNIDAD 6: Control de Accesos e Identidades

- Principios de control de acceso.
- Gestión del ciclo de vida de usuarios.
- Roles, perfiles y privilegios.
- Controles técnicos: autenticación, MFA, contraseñas.
- Accesos privilegiados y cuentas de servicio.
- Revisión periódica y trazabilidad de accesos.

Material Entregable:

- Plantilla "Análisis de Contexto SGSI".
- Matriz PESTEL y FODA editable.
- Mapa de Partes Interesadas.
- Formato de Determinación de Alcance.
- Guía Alignment de madurez contextual.
- Procedimiento "Gobernanza y Gestión".

UNIDAD 7: Gestión de Proveedores y Seguridad en Proyectos

- Evaluación y homologación de proveedores.
- Análisis de riesgos de la cadena de suministro.
- Cláusulas de seguridad y NDA en contratos.
- Monitoreo y auditoría de proveedores críticos.
- Seguridad en proyectos y desarrollo (Security by Design).
- Gestión de terceros con acceso a información sensible.

Material Entregable:

- Plantilla "Matriz de Evaluación de Proveedores".
- Formato de Evaluación de Riesgos de Terceros.
- Cláusulas de seguridad contractual (SLA/NDA).
- Checklist de revisión de proyectos.
- Procedimiento "Gestión de Proveedores".

UNIDAD 8: Gestión de Incidentes y Continuidad Operativa

- Proceso de gestión de incidentes.
- Coordinación con el CSIRT nacional.
- Plan de Continuidad (BCP) y Recuperación (DRP).
- Simulacros de incidentes críticos.
- Comunicación y notificación a autoridades.
- Lecciones aprendidas y mejora post-incidente.

Material Entregable:

- Procedimiento "Gestión de Incidentes SGSI".
- Bitácora de incidentes editable.
- Plantilla "Plan BCP/DRP".
- Checklist de simulacros y validación.
- Guía Alignment de coordinación CSIRT.

UNIDAD 9: Actividades de Soporte del SGSI

- Gestión documental (control, versiones, aprobaciones).
- Administración de recursos y presupuesto SGSI.
- Plan de capacitación y concienciación.
- Matriz de competencias y roles.
- Plan de comunicaciones internas y externas.
- Evaluación del impacto de capacitación y cultura SGSI.

Material Entregable:

- Procedimiento de Control Documental.
- Plantilla "Registro de Documentos Controlados".
- Formato de Gestión de Recursos y Presupuesto.
- Plan de Capacitación Anual SGSI.
- Plantilla de Plan de Comunicaciones.
- Ejemplo: Programa de cultura de seguridad digital.

UNIDAD 10: Evaluación, Auditoría y Mejora Continua

- Auditorías internas basadas en ISO 19011.
- Evaluación del desempeño del SGSI.
- Registro de hallazgos y acciones correctivas.
- Revisión por la dirección.
- Plan de mejora y control de eficacia.
- Preparación para auditoría de certificación.
- Procedimiento de "Revisión por la Dirección"

Material Entregable:

- Checklist de auditoría interna SGSI.
- Plantilla de Informe de Auditoría.
- Plan de Acciones Correctivas.
- Matriz de Madurez SGSI.
- Guía Alignment de mejora continua.
- Procedimiento de "Auditoría Interna"

UNIDAD 11: Simulación Ejecutiva de Gestión de Crisis Cibernética Ante la Caída de

- Escenario práctico: interrupción de un proveedor esencial.
- Activación del Comité de Crisis y roles ejecutivos.
- Coordinación entre continuidad, TI, legal y proveedores.
- Análisis de impacto operativo y comunicación al CSIRT.
- Evaluación de decisiones, tiempos de respuesta y mitigación.
- Redacción del informe post-incidente y plan de mejora.

Material Entregable:

- Guion "Simulación de Crisis - Proveedor".
- Plantilla de registro de decisiones ejecutivas.
- Formato de notificación al CSIRT Nacional.
- Minuta de Comité de Crisis.
- Plantilla de Informe Post-Incidente y Mejora.
- Ejemplo: Caída de proveedor cloud.

UNIDAD 12: Manual Ejecutivo del SGSI de Alignment

- Estructura y contenido del Manual SGSI Alignment.
- Declaración de Aplicabilidad (SoA).
- Consolidación de procesos y evidencias clave.
- Evaluación de madurez y plan de mejora.
- Alineamiento final con la Ley Marco de Ciberseguridad.
- Presentación ejecutiva y cierre del programa.

Material Entregable:

- Plantilla "Manual SGSI Alignment".
- Declaración de Aplicabilidad editable.
- Plantilla de Análisis GAP final.
- Roadmap de madurez 2025-2027.
- Guía Alignment de presentación ejecutiva.

DOCENTE A CARGO



CARLOS LOBOS DE MEDINA

INGENIERO CIVIL EN INFORMÁTICA Y
MAGISTER EN INFORMÁTICA (C) DE LA
UNIVERSIDAD DE SANTIAGO DE CHILE.

Diplomado en Auditoria de Sistemas y
Pos Titulado en Seguridad Computacional
de la Universidad de Chile.



AL FINALIZAR PODRÁ:

- ▶ Implementar un SGSI completo alineado a ISO 27001:2022 y a la Ley Marco de Ciberseguridad.
- ▶ Gestionar incidentes, accesos, proveedores y continuidad con madurez.
- ▶ Desarrollar en una simulación ejecutiva de crisis cibernética realista.
- ▶ Aplicar el Manual Ejecutivo SGSI Alignment con evidencias listas para certificación.
- ▶ Aplicar controles, políticas y procesos con plantillas reales de Alignment.



Quienes han obtenido la **Certificación Alignment** han demostrado poseer de manera efectiva las **Competencias Profesionales** en la implementación, mantenimiento y mejora continua de **Sistemas de Gestión de Seguridad de la Información** conforme a los estándares internacionales vigentes.

VALOR DEL CURSO: \$199.000 Pesos Chilenos (CLP)

El valor corresponde al costo regular actual del curso Implementador Experto ISO 27001 SGSI bajo pago al contado o en cuotas.

¡EXCLUSIVO POR DICIEMBRE!

VALOR PROMOCIONAL:

**2 CURSOS
CERTIFICADOS
X \$299.000**

VALOR REGULAR:

~~1 CURSO: 199.000~~

INICIO: MIÉRCOLES 10 DE DICIEMBRE 2025

COMPRAR LA PROMOCIÓN



¡CONTÁCTANOS!



+569 6769 2920



VENTAS@ALIGNMENT.CL