NewKey

SGSI-ISO 27001

DISEÑO Y PLANIFICACIÓN DE UN SGSI BASADO EN ISO 27001

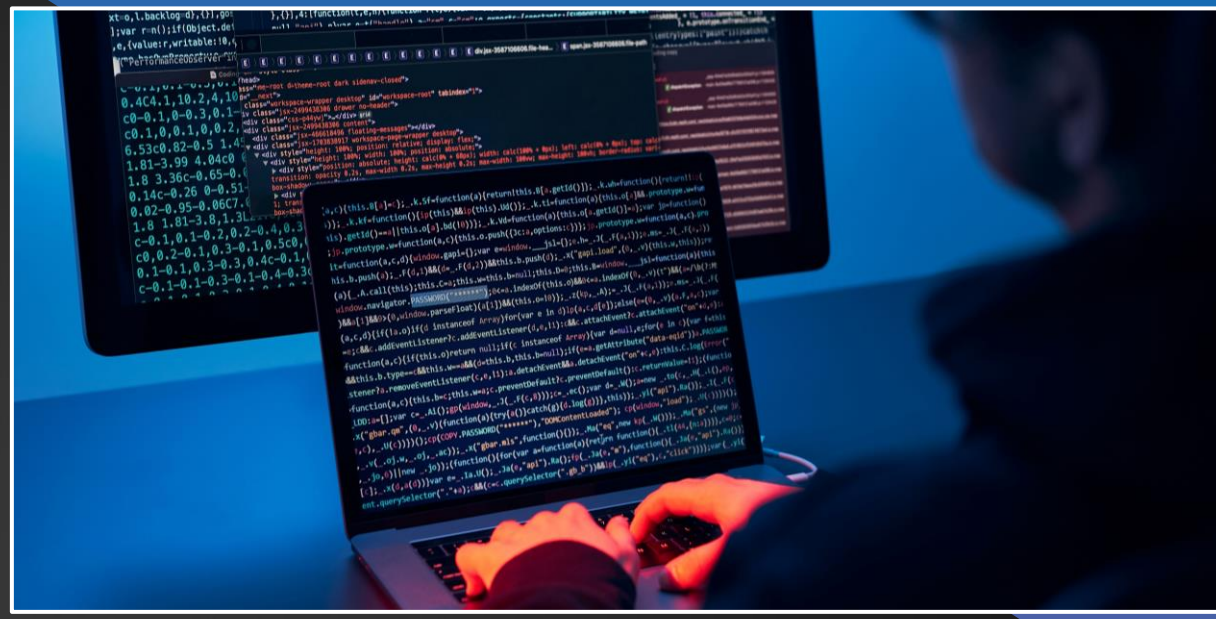
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

GST-101 | ISO 27001

Gen+Asociativo
UN MUNDO DIGITAL A TU ALCANCE

ÍNDICE

- 01. Antecedentes del Curso
- 02. Audiencia
- 03. Metodología
- 04. Objetivos del Curso
- 05. Temario
- 06. Relator



SGSI

Sistema de Gestión de Seguridad de la Información

1. Antecedentes del Curso

El curso ha sido diseñado para proveer la capacidad de gestionar la seguridad de la información basada en el estándar ISO 27001, el que establece que las Organizaciones deben contar con un sistema de gestión de seguridad de la información que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información.

En el curso se entregarán los aspectos estratégicos que permitirán a los participantes del curso comprender al alcance del SGSI y conocer las actividades requeridas para su cumplimiento.

Asimismo, el curso permitirá a los participantes comprender por qué el alcance del SGSI va más allá de los Servicios de Computación e Informática, requiriendo el compromiso del Director del Servicio, sus Directores, Área Jurídica, Contraloría y de Recursos Humanos entre otras.

2. Audiencia

El curso está orientado al personal ejecutivo y técnico responsable por el cumplimiento SGSI:

01 Responsables del Cumplimiento de los SGSI.

02 Responsables de la Auditoría de los SGSI.

03 Jefe de Informática.

04 Oficial de Seguridad. Oficial de Seguridad.

05 Ingenieros de Sistema.

06 Contralores.

07 Auditores.

08 Consultores e Implementadores de SGSI.

3. Metodología

01

Duración del Curso

24 Horas cronológicas distribuidas en 12 sesiones de 2 horas.

02

Modalidad de Impartición

Curso Abierto o Cerrado

- Curso dictado en forma online vía zoom.
- El curso requiere de un mínimo 7 participantes.
- Las sesiones se realizarán en el lugar, fechas y horarios programados
- Las sesiones tienen una orientación teórica y práctica incluyen exposición de temas y discusión del alcance del SGSI en una ronda de preguntas y respuestas.

03

Materiales

A los asistentes del curso se les hace entrega de una carpeta con material original preparado especialmente por **profesionales de experiencia** para el curso. Este material incluye copia de las slides de apoyo a la relatoría del curso y material complementario para el estudio y desarrollo de los contenidos.

NewKey

Gen+Asociativo
UN MUNDO DIGITAL A TU ALCANCE

4. Objetivos del Curso

4.1. Objetivo General

- En este curso se revisan los principales modelos y herramientas que facilitan el proceso de implantación de un sistema de gestión de seguridad de la Información (ISO 27001:2013, ISO 27002:2013) y presentar los conceptos principales correspondientes a la identificación de los activos de una organización y el correspondiente desarrollo, documentación e implementación de políticas, estándares, procedimientos y guías que aseguren la confidencialidad, integridad y disponibilidad de la información a través de una adecuada gestión de riesgos.

  Además, permitirá comprender los conceptos de gestión del riesgo (ISO 27005), comprender y conocer procedimientos, políticas, estándares y guías, conocer la clasificación de la información, conocer responsabilidades y roles en la seguridad de la información.

- Se revisarán su aplicación en el ámbito gubernamental así como los cambios en la nueva versión de la ISO 27002.

4.2. Objetivos Específicos

01

Fundamentos teóricos que avalan la implantación de un SGSI

- Conocer el marco teórico de la seguridad de la información.
- Revisar el conjunto de estándares asociada a la familia ISO 27000.

02

Revisión de la norma ISO 27001 e ISO 27002

- Conocer los 14 dominios de seguridad de la información asociados al estándar ISO 27002 y su contexto en la Organización (estratégico, táctico y operativo).
- Conocer los controles objetivos asociadas a la gestión de seguridad de la información en una organización.
- Revisar el estándar ISO 27001.
- Definir el Alcance asociado a un Sistema de gestión de Seguridad de la Información.
- Conocer las fases asociados a la implantación de un Sistema de Gestión de Seguridad de la Información.

03

SGSI (Sistema de Gestión de Seguridad de la Información)

- Conocer las fases del ciclo de mejoramiento continuo de la Gestión (Planificar, Implantar, Chequear, Mejorar).
- Aplicar el ciclo de mejoramiento continuo a un Sistema de Gestión de Seguridad de la Información.
- Conocer las Políticas de Seguridad de la Información que apoyen la elaboración de un plan de implantación para un Sistema de Gestión de Seguridad de la Información.

4.2. Objetivos Específicos

04

Procesos

- Conocer el estándar ISO 9000 y la norma chile NCH2909-2004.
- Conocer y Revisar una metodología para el levantamiento de procesos.
- Describir la Organización, sus respectivas áreas y los procesos organizacionales.
- Elaborar un Mapa de Proceso.
- Identificar procesos de negocios críticos de la Organización.

05

Activos de Información

- Conocer la metodología de las Elipsis.
- Identificar los Activos de Información.
- Conocer la agrupación de los activos de información.
- Valorizar y administrar los activos de información.

06

Gestión de Riesgos

- Conocer el Estándar ISO 27005.
- Revisar el proceso de gestión de riesgos de Seguridad de la Información.
- Identificar, evaluar y administrar riesgos de seguridad asociados a los activos de información.
- Evaluar Riesgo Inherente.
- Evaluar Riesgo Residual.
- Elaborar la Matriz de Riesgo de Seguridad de la Información.

4.2. Objetivos Específicos

07

Métricas de Seguridad y Plan

- Conocer los niveles de madurez asociados a los controles de seguridad.
- Conocer las métricas que permiten evaluar y revisar el estado de la seguridad de la información.
- Elaborar una presentación del estado de la situación actual de seguridad de la Información.
- Generar un portfolio de proyectos de seguridad.
- Elaborar un Plan de Implantación para un Sistema de Gestión de Seguridad de la Información.

08

SGSI en ámbito Gubernamental y Cambios ISO

- DS-83. PMG-SSI.
- Ciberseguridad.
- Revisar los cambios que se aplicarán en la ISO 27002.

5. Temario

Sección 1: Fundamentos teóricos que avalan la implantación de un SGSI

- Fundamentos de Procesos de Gestión de la Seguridad (Marco Teórico).
- Familia ISO 27000.
- Estándares ISO 27005 asociado a gestión de Riesgos.

Sección 2: Revisión de la norma ISO 27001 e ISO 27002

- Normativa de Seguridad ISO 27002.
- Normativa de Seguridad ISO 27001.

Sección 3: SGSI (Sistema de Gestión de Seguridad de la Información)

- Ciclo de Deming PDCA (Plan-Do-Check-Act).
- Diseño de una guía Metodológica de Implantación de un proceso de Gestión de Seguridad en la Organización.

Sección 4: Procesos

- Elaboración un programa de trabajo para el Levantamiento de los Procesos de la Organización.
- Revisión de los procesos críticos del negocio referidos a los activos de información.

Sección 5: Activos de Información

- Elaboración un Programa de Identificación de Activos de Información
- Valorización de los activos de la Información.

Sección 6: Gestión de Riesgos

- Estándar ISO 27005 gestión de Riesgos.
- Elaboración un Programa Identificación y Evaluación de Riesgos asociados a los activos de la Información.

Sección 7: Métricas de Seguridad y Plan

- Generación de un Análisis Diferencial (estudio de brechas).
- Informe ejecutivo (métricas de seguridad).

Sección 8: SGSI en ámbito Gubernamental y Cambios ISO

- Revisión de normativas tradicionales DS-83, PMG-SSI.
- Revisión de Normativas de Ciberseguridad.
- Infraestructuras Críticas de la Información.
- Revisión de los cambios en la ISO 27002 indicado el borrador 2020.

6. Relator

ERIC JOSÉ DONDERS ORELLANA

- **DIRECTOR** DE NEWKEY (WWW.NEWKEY.CL)
- **ASESOR** EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD
- **CISO** POR 12 AÑOS
- **CISSP** DESDE 2002

+569 82098568

eric.donders@newkey.cl

ericdonderso

6.1. Perfil Profesional

Gen+Asociativo
UN MUNDO DIGITAL A TU ALCANCE

Ingeniero Civil en Computación, con 30 años de experiencia en Gobierno, Gestión, Planificación, Diseño, Desarrollo e Implantación Servicios y Sistemas de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad basada en estándares (Familia ISO 27000, NIST, CIS CSC, PCI/DSS, COBIT 5), Gestión de Riesgos (ISO 31000), Gestión de Continuidad (ISO 22031), Seguridad Aplicativa (OWASP).

Los últimos 5 años capacidad de incorporación y aplicación de nuevas Tecnologías en el ámbito de Cloud (IaaS, PaaS, SaaS) tales como; Amazon Web Services (AWS), Oracle Cloud, MS Azure, Integraciones. Finalmente, el desarrollo de Ciberseguridad en Cloud basado en el Cloud Security Alliance (CSA) y el desarrollo de Servicios basados en Blockchain.
Experiencia en el Diseño e Implantación de Infraestructura de Claves Públicas (PKI) a nivel Organizacional como a nivel Nacional reflejada en la Prestadoras de Servicios de Certificación de Firma Electrónica Avanzada.

Formación consolidada como CISO por 12 años en el Holding Farmacéutico Socofar – Cruz Verde en Chile y Regional (Colombia), además apoyar fuertemente la Gerencia TI Corporativa tanto en el ámbito de Seguridad TI y OT, Infraestructura TI, Proyectos TIC´s y SCADA.
Una alta capacidad para entender el negocio y/o servicios estratégicos de la organización proponiendo estrategias de Seguridad que beneficien el negocio y/o sus objetivos estratégicos.

6.1. Perfil Profesional

Gen+Asociativo
UN MUNDO DIGITAL A TU ALCANCE

Obtención del grado académico de Magister en Seguridad Informática y Protección de la Información, un Diplomado en Aplicaciones Criptográficas, un Postítulo en Seguridad de la Información y la Certificación CISSP desde el año 2002.

Profesor de Postgrado de Magister y Diplomados en Universidades públicas y privadas en temas de Tecnología, Riesgo, Seguridad de Información y Ciberseguridad, por más de 15 años, actualmente profesor en; USACH, Universidad de Chile, Universidad Católica, Universidad Adolfo Ibáñez.

Miembro Fundador y parte de la mesa directiva Capítulo Chileno de ISC2 (2012) y cofundador de la Red Universitaria de Colaboración en Ciberseguridad UCISO (2019).

Ha sido expositor en Conferencias como Secure Chile 2018, CYBERSEC TALKS 2020, y otras organizadas por Capítulo Chileno de ISC2 y Universidades de Chile.

CERTIFICACIONES

- CISSP – (Certified Informativo Systems Security Professionals), Certificación renovada cada 3 años y validada hasta el 2023.
- LA BS7799 – Lead Auditor Information Security (2003).
- CSA - Certified Solaris System Administrator (1998).
- MCSE - Certified Microsoft Certified System Engineer (1997).

PROFESOR/ACADÉMICO UNIVERSITARIO

Actualmente Profesor de Magister y Diplomados en el ámbito de Ciberseguridad y Profesor Guía de Tesis en:

- Universidad Santiago de Chile
- Universidad de Chile
- Universidad Católica
- Universidad Adolfo Ibáñez

SENCE:

Aplicación De Técnicas De Auditoría Interna De Un Sistema De Gestión De Seguridad De La Información Basado En (ISO 27001:2013, ISO 27002:2013).

Código SENCE: 1238034897
Modalidad de instrucción: E-Learning
Modo: Síncrona

www.gen-asociativo.cl

contacto@gen-asociativo.cl
Santiago, Región Metropolitana, Chile