CURSO - TALLER
GESTIÓN DE LA SEGURIDAD DE LA INFORMACION

La Seguridad de la Información según las Normas ISO 27001_02

Instructor: Ing. Daniel De Giorgio, ISO 27001_02_32_35, ISO 22301, SSBB, ITIL –
Duración: 16hs

Un enfoque **aplicable y práctico** con: **casos prácticos reales, juegos** originales de **simulación**, **videos**, ejemplos de **entregables, plantillas** y ejercicios basados en **desafíos cotidianos** que las organizaciones de **nuestro contexto regional** deben resolver, con **la teoría al servicio de la acción**.

OBJETIVO DEL TALLER

Este curso de implementador líder de ISO / IEC 27001 le permite desarrollar la experiencia necesaria para ayudar a una organización a establecer, implementar, administrar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO / IEC 27001. Durante este curso de capacitación, también obtendrá una comprensión profunda de las mejores prácticas de los sistemas de gestión de seguridad de la información para proteger la información confidencial de la organización y mejorar el rendimiento y la eficacia generales.

Recorre las mejores prácticas de Seguridad de la Información y las etapas necesarias para desarrollar y comprender el proceso del SGSI, incluyendo los pasos críticos necesarios para lograr una comprensión profunda de la naturaleza y las necesidades de funcionamiento de una Organización, la identificación e implementación de estrategias, cambios en la estructura de la organización y procesos de negocio.

Utilizando casos de estudio basados en escenarios de la vida real, los asistentes adquirirán conocimientos prácticos sobre cómo llevar a cabo una implementación de un SGSI. Permite a los asistentes beneficiarse de un ambiente de aprendizaje dinámico, donde la interacción entre pares fortalece la adquisición de conocimientos a través del intercambio de ideas y experiencias de la vida real.

DESTINATARIOS

Profesionales de las áreas de Seguridad de la Información, Continuidad del Negocio, Riesgos Tecnológicos/Operacionales, Auditoría, Tecnología y Sistemas, Procesos y Cumplimiento. Consultores y Profesionales involucrados en implementar un Programa de Seguridad de la Información en sus Organizaciones.

- Gerentes o consultores involucrados en la Gestión de la Seguridad de la Información.
- Asesores expertos que buscan dominar la implementación de un Sistema de Gestión de la Seguridad de la Información.
- Personas responsables de mantener la conformidad con los requisitos del SGSI.
- Miembros del equipo del SGSI

TEMARIO

❖ Introducción a ISO 27001 y el Sistema de Gestión de Seguridad de la Información

1. **Presentación, Objetivos y Programa del Curso**
    a. Cuestiones generales
    b. Objetivos del curso
    c. Programa del curso
2. **Estándar y marco regulatorio**
    a. Estructura de la ISO
    b. Principios fundamentales de la ISO
    c. Estándares de Seguridad de la Información
    d. La familia ISO 27000
    e. Marco regulatorio integrado
    f. Estándares de Gestión de Proyectos
3. **Sección 3: Sistema de Gestión de SI (SGSI)**
    a. Definición del SGSI
    b. Enfoque en los procesos
    c. Visión general. Cláusulas 4 a 10
    d. Anexo A
4. **Sección 4: Principios fundamentales de la Seguridad de la Información**
    a. Activo y activo de información
    b. Seguridad de la Información
    c. Confidencialidad, integridad y disponibilidad
    d. Vulnerabilidad, amenaza e impacto
    e. Riesgo para la Seguridad de la Información
    f. Objetivos y controles de seguridad
    g. Clasificación de controles de seguridad
5. **Sección 5: Iniciando la implementación del SGSI**
    a. Enfoque para la Implementación del SGSI
    b. Metodología de implementación del SGSI
    c. Mejores prácticas en la gestión de proyectos

d. Alineación con las mejores prácticas

Sección 6: Descripción de la Organización y clarificación de los objetivos de SI

a. Comprensión de la Organización
b. Identificación y análisis de las partes interesadas
c. Identificación y análisis de los requisitos y expectativas
d. Determinación de los objetivos
e. Definición preliminar del alcance

Sección 7: Análisis del Sistema de Gestión existente

a. Recopilación de la información
b. Realización de una entrevista
c. Análisis de brechas

❖ Capítulo 2: Planificar la Implementación de un SGSI

Sección 8: Liderazgo y aprobación del Proyecto SGSI

a. Caso de Negocio
b. Equipo de proyecto
c. Plan de proyecto
d. Autorización de la Dirección

Sección 9: Alcance del SGSI

a. Definir los límites de la organización
b. Definir los límites de los sistemas de información
c. Definir el ámbito y límites físicos
d. Definir el alcance del SGSI
e. Cambios en el alcance
f. Extensión del ámbito de aplicación

Sección 10: Políticas de SI

a. Tipos de políticas
b. Modelos y estructuras de una política
c. Políticas del SGSI
d. Política de Seguridad de la Información
e. Políticas específicas
f. Proceso de Gestión de Políticas

Sección 11: Evaluación de Riesgos

a. El estándar ISO 27005
b. Enfoque para la evaluación de riesgos
c. Metodología para la evaluación de riesgos
d. Identificación de riesgos
e. Estimación de riesgos
f. Evaluación de riesgos
g. Tratamiento de riesgos
h. Aceptación de riesgos

Sección 12: Declaración de Aplicabilidad y autorización de la Dirección para aplicar el SGSI

a. Revisión y selección de objetivos y controles
b. Controles de seguridad obligatorios

c. Justificación de los controles elegidos
d. Justificación de controles excluidos
e. Elaboración de la declaración de aplicabilidad
f. Autorización de la Dirección para aplicar el SGSI

Sección 13: Definición de la estructura organizativa de SI

a. Estructura organizativa
b. Funciones y responsabilidades de las partes interesadas
c. Proceso de gestión de autorización
d. Funciones y responsabilidades de los comités

❖ Capítulo 3: Despliegue del SGSI

Sección 14: Definición del proceso de gestión de documentos

a. Creación de plantillas
b. Gestión de documentos
c. Implementación de un sistema de gestión de documentos
d. Gestión de registros
e. Lista maestra de documentos

Sección 15: Diseño de Controles de seguridad y elaboración de políticas y procedimientos específicos

a. Diseño de los procesos y controles
b. Descripción de los procesos y controles
c. Redacción de políticas específicas
d. Procedimientos de escritura
e. Definición de los registros

Sección 16: Plan de Comunicación

a. Principios de una estrategia de comunicación eficaz
b. Proceso de comunicación de Seguridad de la Información
c. Establecer objetivos de comunicación
d. Identificas las partes interesadas
e. Planificar las actividades de comunicación
f. Realizar una actividad de comunicación
g. Evaluar la comunicación

Sección 17: Plan de Capacitación y Sensibilización

a. Definición de las competencias y la capacitación
b. Diferencia entre capacitación, sensibilización y comunicación
c. Definir necesidades de capacitación
d. Diseño y planificación de la capacitación
e. Provisión de la capacitación
f. Evaluación de los resultados de la capacitación

Sección 18: Implementación de Controles de Seguridad

a. Implementación de procesos y controles de Seguridad
b. Introducción de los controles del Anexo A

Sección 19: Gestión de Incidentes

a. Política de Gestión de Incidentes
b. Procesos y procedimientos de Gestión de Incidentes

c. Equipo de Respuesta a Incidentes
d. Controles de seguridad relacionados con la Gestión de Incidentes
e. Proceso forense
f. Registro de incidentes de seguridad
g. Medida y revisión del proceso de Gestión de Incidentes

Sección 20: Gestión de Operaciones

a. Planificación de la gestión de cambio
b. Transferencia de Operaciones
c. Gestión de recursos necesarios para mantener el SGSI

Capítulo 4: Monitoreo del SGSI, mejora continua

Sección 21: Supervisión, Medición, Análisis y Evaluación

a. Objetivos de la medición
b. Programa de medición Seguridad de la Información
c. Desarrollo de indicadores de Seguridad de la Información
d. Documentación de los indicadores
e. Cuadro de mandos de Seguridad de la Información

Sección 22: Auditoría Interna

a. Las diferencias entre las Auditorías Internas y Externas
b. Rol de la Función de Auditoría Interna
c. Independencia, objetividad e imparcialidad
d. Planificación de las actividades de auditoría
e. Crear un procedimiento de auditoría
f. Realizar actividades de auditoría
g. Actividades de seguimiento de no conformidades

Sección 23: Revisión por la Dirección

a. Preparación de la revisión por la Dirección
b. La realización de una revisión por la Dirección
c. Cierre de la revisión por la Dirección
d. Actividades de seguimiento de la revisión por la Dirección

Sección 24: Tratamiento de problemas y no conformidades

a. Proceso de análisis de la causa raíz
b. Herramienta de análisis de la causa raíz
c. Procedimiento de acciones correctivas y preventivas

Sección 25: Mejora Continua

a. Proceso de seguimiento continuo de factores de cambio
b. Mantenimiento y mejora del SGSI
c. Actualización continua de la documentación y registros
d. Documentar las mejoras

DESAFIOS FRECUENTES ABORDADOS POR EL TALLER:

- **Síndrome de la hoja en blanco:** dificultades para empezar a construir y gestionar un Análisis de Impacto al Negocio sólido.

- **Alcances desmedidos:** expectativas de querer analizar todos los impactos a todos los activos.
- **El enemigo interior:** silos y solapamientos entre áreas, culturas organizacionales nocivas ("esto no va a pasarnos a nosotros").
- **La obsesión teórica:** metodologías que brillan en el PDF y se apagan al aplicarlas en la realidad.
- **La trampa del pasado:** gestionando el Programa ignorando expectativas, tendencias y necesidades de las partes interesadas.
- **Enfoques estáticos** (para amenazas dinámicas): el peligro de la foto desactualizada y la "falsa sensación de seguridad".
- **Percepción negativa:** la Seguridad de la Información vista como un gasto o solo para cumplir.
- **Des-Integración:** inconsistencias con objetivos, necesidades y prioridades del Negocio.
- **La verdad incómoda:** dificultades para exponer los resultados y necesidades de un Programa de Seguridad a la Alta Gerencia.

PERFIL DEL INSTRUCTOR: Ing. Daniel De Giorgio, MBCI, ISO LI&LA, SSBB, ITIL:

- Ingeniero Electrónico (UBA).
- Instructor certificado y profesional certificado del Business Continuity Institute UK(BCI).
- Instructor certificado y profesional certificado (Implementador Líder y Auditor Líder) de las normas internacionales ISO-22301, ISO-22317, ISO 22316, ISO 27001, ISO 27002, ISO 27035, ISO-27031 e ISO-27032.
- Asesor Certificado del Modelo de Madurez BCMM © de Virtual Corporation (USA).
- Profesional Certificado Six Sigma Black Belt.
- Profesional Certificado ITIL.
- Profesor universitario invitado en la Maestría de Seguridad de la Información de la Universidad Nacional de Buenos Aires.
- Cuenta con 38 años de experiencia profesional en Tecnologías de la Información y Comunicaciones (TIC) y en la Implementación y Gestión de Programas de Continuidad del Negocio en la industria financiera.
- Disertante en Congresos Internacionales en temas de Continuidad del Negocio.
- Amplia trayectoria en Latinoamérica brindando talleres in-company para distintas industrias.
- Experiencia profesional en Latinoamérica en consultoría sobre las temáticas abordadas en el taller.
- Ha implementado exitosamente Sistemas de Gestión de Seguridad de la Información y Continuidad del Negocio en entidades financieras de la República Argentina y asesora empresas en implementaciones de BCM.
- Director del BCI Regional Forum Argentina.
- Miembro del Comité Editorial del Disaster Recovery Journal en español.
- Miembro de la Junta Directiva de ALCONT (Asociación Latinoamericana de Continuidad de Negocio).
- Miembro del Comité Académico de Usuaria (Asociación Argentina de Usuarios de la Informática y las Telecomunicaciones).
- Miembro #17762 del Business Continuity Institute UK).