ACADEMIA INTEGRAL
CENTRO DE NUEVAS TECNOLOGIAS

LA FORMACIÓN ES LA CLAVE DEL ÉXITO

Guía del Curso
Técnico Profesional en Sistema de Gestión de Seguridad de la Información UNE-ISO/IEC 27001:2017

Modalidad de realización del curso: A distancia y Online
Titulación: Diploma acreditativo con las horas del curso

OBJETIVOS

La adecuada implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) permite asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones. Este curso, dirigido a quienes decidan encaminar su carrera profesional al incipiente mercado de la certificación, gestión y auditoría de la calidad, ofrece los conocimientos básicos para la aplicación de la Norma ISO/IEC 27001 dentro de su organización, así como las pautas para implementar un SGSI según el estándar ISO/IEC 27001, siguiendo los controles recomendados por el estándar ISO/IEC 27002 en sus respectivas cláusulas.

CONTENIDOS

MÓDULO 1. LA SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 1. NATURALEZA Y DESARROLLO DE LA SEGURIDAD DE LA INFORMACIÓN

1. La sociedad de la información
2. ¿Qué es la seguridad de la información?
3. Importancia de la seguridad de la información
4. Principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad
5. - Principio Básico de Confidencialidad
6. - Principio Básico de Integridad
7. - Disponibilidad
8. Descripción de los riesgos de la seguridad
9. Selección de controles
10. Factores de éxito en la seguridad de la información

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE SEGURIDAD DE LA INFORMACIÓN

1. Marco legal y jurídico de la seguridad de la información
2. Normativa comunitaria sobre seguridad de la información
3. - Planes de acción para la utilización más segura de Internet
4. - Estrategias para una sociedad de la información más segura
5. - Ataques contra los sistemas de información
6. - La lucha contra los delitos informáticos
7. - La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
8. Normas sobre gestión de la seguridad de la información: Familia de Normas ISO 27000
9. - Familia de Normas ISO 27000
10. - Norma ISO/IEC 27002:2009
11. Legislación española sobre seguridad de la información
12. - La protección de datos de carácter personal
13. - La Ley Orgánica - de 13 de diciembre, de Protección de Datos de Carácter Personal

14. - El Real Decreto - de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica - de 13 de diciembre, de protección de datos de carácter personal
15. - La Agencia Española de Protección de Datos
16. - El Real Decreto - de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
17. - Ley - de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
18. - La Ley - de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico
19. - La Ley - de 9 de mayo, General de Telecomunicaciones
20. - La Ley - de 19 de diciembre, de firma electrónica
21. - La Ley de propiedad intelectual
22. - La Ley de propiedad industrial

UNIDAD DIDÁCTICA 3. BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN: NORMA ISO/IEC 27002

1. Aproximación a la norma ISO/IEC 27002
2. Alcance de la Norma ISO/IEC 27002
3. Estructura de la Norma ISO/IEC 27002
4. - Las cláusulas del control de seguridad
5. - Las principales categorías de seguridad
6. Evaluación y tratamiento de los riesgos de seguridad
7. - Evaluación de los riesgos de seguridad
8. - Tratamiento de los riesgos de seguridad

UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD, ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE ACTIVOS

1. Política de seguridad de la información
2. - Etapas en el desarrollo de una política de seguridad de la información

3. - Características esenciales de una política de seguridad de la información
4. - Documento de política de la seguridad de la información
5. - Revisión de la política de seguridad de la información
6. Organización de la seguridad de la información
7. Organización interna de la seguridad de la información
8. - Compromiso de la dirección con la seguridad de la información
9. - Coordinación de la seguridad de la información
10. - Asignación de responsabilidad de seguridad de la información
11. - Autorización de procesos para facilidades procesadoras de la información
12. - Acuerdos de confidencialidad para la protección de la información
13. - Contacto con las autoridades y con grupos de interés especial en los incidentes de seguridad
14. - Revisión independiente de la seguridad de la información
15. Grupos o personas externas: el control de acceso a terceros
16. - Identificación de los riesgos de seguridad relacionados con personas externas
17. - Tratamiento de la seguridad de la información en las relaciones con los clientes
18. - Tratamiento de la seguridad de la información en acuerdos con terceros
19. Clasificación y control de activos de seguridad de la información
20. Responsabilidad por los activos de seguridad de la información
21. - Inventario de los activos de seguridad de la información
22. - Propiedad de los activos de seguridad de la información
23. - Uso aceptable de los activos de seguridad de la información
24. Clasificación de la información
25. - Lineamientos de clasificación de la información
26. - Etiquetado y manejo de información

UNIDAD DIDÁCTICA 5. SEGURIDAD FÍSICA, AMBIENTAL Y DE LOS RECURSOS HUMANOS

1. Seguridad de la información ligada a los recursos humanos
2. Medidas de seguridad de la información antes del empleo
3. - Establecimiento de roles y responsabilidades de los candidatos
4. - Investigación de antecedentes de los candidatos para el empleo

5. - Términos y condiciones del empleo
6. Medidas de seguridad de la información durante el empleo
7. - Responsabilidades de la gerencia o dirección de la organización
8. - Conocimiento, educación y capacitación en seguridad de la información
9. - Incumplimiento de las previsiones relativas a la seguridad de la información: el proceso disciplinario
10. Seguridad de la información en la finalización de la relación laboral o cambio de puesto de trabajo
11. - Responsabilidades de terminación
12. - Devolución de los activos
13. - Cancelación de los derechos de acceso a la información
14. Seguridad de la información ligada a la seguridad física y ambiental o del entorno
15. Las áreas seguras
16. - El perímetro de seguridad física
17. - Los controles de ingreso físico
18. - Seguridad de oficinas, locales, habitaciones y medios
19. - Protección contra amenazas internas y externas a la información
20. - El trabajo en áreas aseguradas
21. - Áreas de carga y descarga
22. Los equipos de seguridad
23. - Seguridad en el emplazamiento y protección de equipos
24. - Instalaciones de suministro seguras
25. - Protección del cableado de energía y telecomunicaciones
26. - Mantenimiento de los equipos
27. - Seguridad de los equipos fuera de las instalaciones
28. - Reutilización o retirada segura de equipos
29. - Retirada de materiales propiedad de la empresa
30. - Equipo de usuario desatendido
31. - Política de puesto de trabajo despejado y pantalla limpia

UNIDAD DIDÁCTICA 6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

1. Aproximación a la gestión de las comunicaciones y operaciones
2. Procedimientos y responsabilidades operacionales
3. - Documentación de los procesos de operación
4. - La gestión de cambios en los medios y sistemas de procesamiento de información
5. - Gestión de capacidades
6. - Separación de los recursos de desarrollo, prueba y operación para reducir los riesgos de acceso no autorizado
7. Gestión de la prestación de servicios de terceras partes
8. - Política de seguridad de la información en las relaciones con los proveedores
9. - Requisitos de seguridad en contrato con terceros
10. - Cadena de suministros de tecnología de la información y de las comunicaciones
11. Planificación y aceptación del sistema
12. - Políticas para la seguridad de la información
13. - Revisión de las políticas para la seguridad de la información
14. Protección contra códigos maliciosos y móviles
15. - Controles contra el código malicioso
16. - Control contra códigos móviles
17. Copias de seguridad de la información
18. Gestión de la seguridad de la red
19. - Los controles de red
20. - La seguridad de los servicios de red
21. - Segregación en redes
22. Gestión de medios
23. - Gestión de medios removibles o extraíbles
24. - Eliminación de soportes o medios
25. - Soportes físicos en tránsito
26. - La seguridad de la documentación del sistema
27. El intercambio de información
28. - Políticas y procedimientos de intercambio de información
29. - Acuerdos de intercambio
30. - Seguridad de los soportes físicos en tránsito
31. - Mensajería electrónica
32. - Acuerdos de confidencialidad o no revelación

33. Los servicios de comercio electrónico
34. - Información relativa al comercio electrónico
35. - Las transacciones en línea
36. - La seguridad de la información puesta a disposición pública
37. Supervisión para la detección de actividades no autorizadas
38. - Registro de eventos
39. - Protección de la información de los registros
40. - La protección de la información de los registros
41. - Sincronización de reloj

UNIDAD DIDÁCTICA 7. EL CONTROL DE ACCESOS A LA INFORMACIÓN

1. El control de accesos: generalidades, alcance y objetivos
2. Requisitos de negocio para el control de accesos
3. - Política de control de acceso
4. Gestión de acceso de usuario
5. - Registro del usuario
6. - Gestión o administración de privilegios
7. - Gestión de contraseñas de usuario
8. - Revisión de los derechos de acceso de usuario
9. Responsabilidades del usuario
10. - El uso de contraseñas
11. - Protección de equipos desatendidos
12. - Política de puesto de trabajo despejado y pantalla limpia
13. Control de acceso a la red
14. - La política de uso de los servicios en red
15. - Autentificación de los usuarios de conexiones externas
16. - Identificación de equipos en las redes
17. - Diagnóstico remoto y protección de los puertos de configuración
18. - Segregación de las redes
19. - Control de la conexión a la red
20. - El control de routing o encaminamiento de red
21. Control de acceso al sistema operativo

22. - Procedimientos seguros de inicio de sesión
23. - Identificación y autentificación del usuario
24. - El sistema de gestión de contraseñas
25. - El uso de los recursos del sistema
26. - La desconexión automática de sesión
27. - Limitación del tiempo de conexión
28. Control de acceso a las aplicaciones y a la información
29. - Restricciones del acceso a la información
30. - Aislamiento de sistemas sensibles
31. Informática móvil y teletrabajo
32. - Los ordenadores portátiles y las comunicaciones móviles
33. - El teletrabajo

UNIDAD DIDÁCTICA 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

1. Objetivos del desarrollo y mantenimiento de sistemas de información
2. Requisitos de seguridad de los sistemas de información
3. Tratamiento correcto de la información en las aplicaciones
4. - Validación de los datos de entrada
5. - El control de procesamiento interno
6. - La integridad de los mensajes
7. - Validación de los datos de salida
8. Controles criptográficos
9. - Política de uso de los controles criptográficos
10. - Gestión de claves
11. Seguridad de los archivos del sistema
12. - Control del software en explotación
13. - Protección de los datos de prueba en el sistema
14. - El control de acceso al código fuente de los programas
15. Seguridad de los procesos de desarrollo y soporte
16. - Procedimientos para el control de cambios
17. - Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo

18. - Restricciones a los cambios en los paquetes de software
19. - Entorno de desarrollo seguro
20. - Externalización de software por terceros
21. Gestión de la vulnerabilidad técnica

UNIDAD DIDÁCTICA 9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN Y DE LA CONTINUIDAD DEL NEGOCIO

1. La gestión de incidentes en la seguridad de la información
2. Notificación de eventos y puntos débiles en la seguridad de la información
3. - Notificación de los eventos en la seguridad de la información
4. - Notificación de puntos débiles de la seguridad
5. Gestión de incidentes y mejoras en la seguridad de la información
6. - Responsabilidades y procedimientos
7. - Aprendizaje de los incidentes de seguridad de la información
8. - Recopilación de evidencias
9. Gestión de la continuidad del negocio
10. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio
11. - Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
12. - Continuidad del negocio y evaluación de riesgos
13. - Desarrollo e implantación de planes de continuidad del negocio que incluyan la seguridad de la información
14. - Marco de referencia para la planificación de la continuidad del negocio
15. - Pruebas, mantenimiento y reevaluación de los planes de continuidad

UNIDAD DIDÁCTICA 10. CUMPLIMIENTO DE LAS PREVISIONES LEGALES Y TÉCNICAS

1. Cumplimiento de los requisitos legales
2. - Normativa aplicable
3. - Derechos de propiedad intelectual

4. - Protección de registros organizacionales
5. - Privacidad de la información personal
6. - Prevención del mal uso de los medios de procesamiento de la información
7. - Regulación de los controles criptográficos
8. Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico
9. - Cumplimiento de las políticas y estándares de seguridad
10. - Verificación del cumplimiento técnico
11. Consideraciones de la auditoría de los sistemas de información
12. - Controles de auditoría de los sistemas de información
13. - Protección de las herramientas de auditoría de los sistemas de información

MÓDULO 2. EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 11. LA NORMA UNE-EN-ISO/IEC 27001:2017

1. Objeto y ámbito de aplicación
2. Relación con la Norma ISO/IEC 27002:2009
3. Definiciones y términos de referencia
4. Beneficios aportados por un sistema de seguridad de la información
5. Introducción a los sistemas de gestión de seguridad de la información

UNIDAD DIDÁCTICA 12. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN

1. Contexto
2. Liderazgo
3. Planificación
4. - Acciones para tratar los riesgos y oportunidades
5. - Objetivos de seguridad de la información y planificación para su consecución
6. Soporte

UNIDAD DIDÁCTICA 13. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

1. Operación
2. Evaluación del desempeño
3. - Seguimiento, medición, análisis y evaluación
4. - Auditoría interna
5. - Revisión por la dirección
6. Mejora
7. - No conformidad y acciones correctivas
8. - Mejora continua

C/ San Lorenzo 2 - 2
29001 Málaga

Tlf: 952 215 476
Fax: 951 987 941

www.academiaintegral.com.es
E-mail: info@academiaintegral.com.es

ACADEMIA INTEGRAL
CENTRO DE NUEVAS TECNOLOGIAS