



**Máster en implantación, gestión y
auditoría de sistemas de seguridad
de información ISO 27001 –
ISO 27002**



Working

Formación Integral S.L.

www.workingformacion.com

OBJETIVOS

Este Master en Implantación, Gestión y Auditoría de Sistemas de Seguridad de Información ISO 27001-ISO 27002 le ofrece una formación especializada en la materia. Hoy en día la seguridad informática es un tema muy importante y sensible, que abarca un gran conjunto de aspectos en continuo cambio y constante evolución, que exige que los profesionales informáticos posean conocimientos totalmente actualizados. Así, la Norma UNE-ISO/IEC 27001: 2014 está elaborada para emplearse en cualquier tipo de organización. La adecuada y correcta implementación de un SGSI permite a las empresas asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. El presente Master en Implantación, Gestión y Auditoría de Sistemas de Seguridad de Información ISO 27001-ISO 27002 pretende formar al alumnado a nivel teórico-práctico en el desempeño de todas estas funciones.

CONTENIDOS

MÓDULO 1 – 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. Autenticación 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 autenticación 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

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

MÓDULO 2 – SEGURIDAD EN EQUIPOS INFORMÁTICOS

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
2. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
3. Salvaguardas y tecnologías de seguridad más habituales
4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

1. Identificación de procesos de negocio soportados por sistemas de información
2. Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
3. Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

1. Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
2. Metodologías comúnmente aceptadas de identificación y análisis de riesgos
3. Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1. Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.

2. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
3. Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Principios generales de protección de datos de carácter personal
2. Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
3. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
4. Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

1. Determinación de los perímetros de seguridad física
2. Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
3. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
4. Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
5. Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
6. Elaboración de la normativa de seguridad física e industrial para la organización

7. Sistemas de ficheros más frecuentemente utilizados
8. Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
9. Configuración de políticas y directivas del directorio de usuarios
10. Establecimiento de las listas de control de acceso (ACLs) a ficheros
11. Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
12. Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
13. Sistemas de autenticación de usuarios débiles, fuertes y biométricos
14. Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
15. Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

1. Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
2. Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
3. Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

UNIDAD DIDÁCTICA 8. ROBUSTECIMIENTO DE SISTEMAS

1. Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información

2. Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
3. Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
4. Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
5. Actualización de parches de seguridad de los sistemas informáticos
6. Protección de los sistemas de información frente a código malicioso
7. Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
8. Monitorización de la seguridad y el uso adecuado de los sistemas de información

UNIDAD DIDÁCTICA 9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

1. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
2. Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
3. Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
4. Definición de reglas de corte en los cortafuegos
5. Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6. Establecimiento de la monitorización y pruebas del cortafuegos

MÓDULO 3 - AUDITORÍA DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

1. Código deontológico de la función de auditoría
2. Relación de los distintos tipos de auditoría en el marco de los sistemas de información
3. Criterios a seguir para la composición del equipo auditor
4. Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
5. Tipos de muestreo a aplicar durante el proceso de auditoría
6. Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
7. Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
8. Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
9. Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

UNIDAD DIDÁCTICA 2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Principios generales de protección de datos de carácter personal
2. Normativa europea recogida en la directiva 95/46/CE
3. Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
4. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
5. Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
6. Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de

carácter personal

UNIDAD DIDÁCTICA 3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

1. Introducción al análisis de riesgos
2. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
3. Particularidades de los distintos tipos de código malicioso
4. Principales elementos del análisis de riesgos y sus modelos de relaciones
5. Metodologías cualitativas y cuantitativas de análisis de riesgos
6. Identificación de los activos involucrados en el análisis de riesgos y su valoración
7. Identificación de las amenazas que pueden afectar a los activos identificados previamente
8. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
9. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
10. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
11. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
12. Determinación de la probabilidad e impacto de materialización de los escenarios
13. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
14. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no

15. Relación de las distintas alternativas de gestión de riesgos
16. Guía para la elaboración del plan de gestión de riesgos
17. Exposición de la metodología NIST SP 800-30
18. Exposición de la metodología Magerit versión 2

UNIDAD DIDÁCTICA 4. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

1. Herramientas del sistema operativo tipo Ping, Traceroute, etc
2. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
3. Herramientas de análisis de vulnerabilidades tipo Nessus
4. Analizadores de protocolos tipo WireShark, DSniff, Cain Abel, etc.
5. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
6. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

UNIDAD DIDÁCTICA 5. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS.

1. Principios generales de cortafuegos
2. Componentes de un cortafuegos de red
3. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
4. Arquitecturas de cortafuegos de red
5. Otras arquitecturas de cortafuegos de red

UNIDAD DIDÁCTICA 6. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

1. Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

2. Guía para la elaboración del plan de auditoría
3. Guía para las pruebas de auditoría
4. Guía para la elaboración del informe de auditoría

MÓDULO 4 -. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2. Identificación y caracterización de los datos de funcionamiento del sistema
3. Arquitecturas más frecuentes de los sistemas de detección de intrusos
4. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5. Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1. Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL DE CÓDIGO MALICIOSO

1. Sistemas de detección y contención de código malicioso
2. Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
3. Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
5. Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso
7. Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1. Procedimiento de recolección de información relacionada con incidentes de seguridad
2. Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
3. Proceso de verificación de la intrusión
4. Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

UNIDAD DIDÁCTICA 5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1. Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
2. Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
3. Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
4. Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
5. Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
6. Establecimiento del nivel de intervención requerido en función del impacto previsible
7. Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones
8. Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
9. Proceso para la comunicación del incidente a terceros, si procede
10. Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1. Conceptos generales y objetivos del análisis forense
2. Exposición del Principio de Lockard
3. Guía para la recogida de evidencias electrónicas:
4. Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados

5. Guía para la selección de las herramientas de análisis forense

MÓDULO 5. SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

UNIDAD DIDÁCTICA 1. CRIPTOGRAFÍA

1. Perspectiva histórica y objetivos de la criptografía
2. Teoría de la información
3. Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos
4. Elementos fundamentales de la criptografía de clave privada y de clave pública
5. Características y atributos de los certificados digitales
6. Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente
7. Algoritmos criptográficos más frecuentemente utilizados
8. Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización
9. Elementos fundamentales de las funciones resumen y los criterios para su utilización
10. Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica
11. Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización
12. Criterios para la utilización de técnicas de cifrado de flujo y de bloque
13. Protocolos de intercambio de claves
14. Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop

UNIDAD DIDÁCTICA 2. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. Identificación de los componentes de una PKI y su modelo de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructura de gestión de privilegios (PMI)
7. Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales
8. Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 3. COMUNICACIONES SEGURAS

1. Definición, finalidad y funcionalidad de redes privadas virtuales
2. Protocolo IPSec
3. Protocolos SSL y SSH
4. Sistemas SSL VPN
5. Túneles cifrados
6. Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN

MÓDULO 6. GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UNIDAD DIDÁCTICA 1. GESTIÓN DE LA SEGURIDAD Y NORMATIVAS

1. Metodología ITIL Librería de infraestructuras de las tecnologías de la información
2. Ley orgánica de protección de datos de carácter personal.
3. Normativas más frecuentemente utilizadas para la gestión de la seguridad física

UNIDAD DIDÁCTICA 2. ANÁLISIS DE LOS PROCESOS DE SISTEMAS

1. Identificación de procesos de negocio soportados por sistemas de información
2. Características fundamentales de los procesos electrónicos
3. Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
4. Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
5. Técnicas utilizadas para la gestión del consumo de recursos

UNIDAD DIDÁCTICA 3. DEMOSTRACIÓN DE SISTEMAS DE ALMACENAMIENTO

1. Tipos de dispositivos de almacenamiento más frecuentes
2. Características de los sistemas de archivo disponibles
3. Organización y estructura general de almacenamiento
4. Herramientas del sistema para gestión de dispositivos de almacenamiento

UNIDAD DIDÁCTICA 4. UTILIZACIÓN DE MÉTRICAS E INDICADORES DE MONITORIZACIÓN DE RENDIMIENTO DE SISTEMAS

1. Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
2. Identificación de los objetos para los cuales es necesario obtener indicadores
3. Aspectos a definir para la selección y definición de indicadores
4. Establecimiento de los umbrales de rendimiento de los sistemas de información
5. Recolección y análisis de los datos aportados por los indicadores

6. Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

UNIDAD DIDÁCTICA 5. CONFECCIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

1. Identificación de los dispositivos de comunicaciones
2. Análisis de los protocolos y servicios de comunicaciones
3. Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
4. Procesos de monitorización y respuesta
5. Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
6. Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
7. Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
8. Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

UNIDAD DIDÁCTICA 6. SELECCIÓN DEL SISTEMA DE REGISTRO DE EN FUNCIÓN DE LOS REQUERIMIENTOS DE LA ORGANIZACIÓN

1. Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
2. Análisis de los requerimientos legales en referencia al registro
3. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
4. Asignación de responsabilidades para la gestión del registro
5. Alternativas de almacenamiento para los registros del sistema y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad

6. Guía para la selección del sistema de almacenamiento y custodia de registros

UNIDAD DIDÁCTICA 7. ADMINISTRACIÓN DEL CONTROL DE ACCESOS ADECUADOS DE LOS SISTEMAS DE INFORMACIÓN

1. Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
2. Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
3. Requerimientos legales en referencia al control de accesos y asignación de privilegios
4. Perfiles de de acceso en relación con los roles funcionales del personal de la organización
5. Herramientas de directorio activo y servidores LDAP en general
6. Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
7. Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

MODALIDAD

METODOLOGÍA

Online. Se entrega el material a través de nuestra plataforma virtual homologada. Contará con acceso a la misma las 24 horas al día los 365 días a la semana.

<http://cursosonline.workingformacion.com>

IMPARTIDO POR

Tutor experto en la materia. Contará con apoyo a través de nuestra plataforma en todo momento.

Al finalizar el curso se hará entrega de un
DIPLOMA HOMOLOGADO





Working

Formación Integral S.L.

Paseo Rosales 32, local 9 50008 Zaragoza
976 242 109 - info@workingformacion.com

www.workingformacion.com

