Curso Online. Técnico en Seguridad Informática

Working
Formación Integral S.L.

www.workingformacion.com

OBJETIVOS

La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

CONTENIDOS

MÓDULO 1. SEGURIDAD INFORMATICA

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

5. Identificación de procesos de negocio soportados por sistemas de información
6. Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
7. Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

8. Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
9. Metodologías comúnmente aceptadas de identificación y análisis de riesgos

10. Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

11. 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
12. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
13. Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

14. Principios generales de protección de datos de carácter personal
15. Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
16. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
17. 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

18. Determinación de los perímetros de seguridad física
19. 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

20. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
21. Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
22. Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
23. Elaboración de la normativa de seguridad física e industrial para la organización
24. Sistemas de ficheros más frecuentemente utilizados
25. Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
26. Configuración de políticas y directivas del directorio de usuarios
27. Establecimiento de las listas de control de acceso (ACLs) a ficheros
28. Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
29. Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
30. Sistemas de autenticación de usuarios débiles, fuertes y biométricos
31. Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
32. Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

33. Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
34. Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

35. 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. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

36. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
37. Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
38. Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
39. Definición de reglas de corte en los cortafuegos
40. Relación de los registros de auditoría del cortafuegos necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
41. Establecimiento de la monitorización y pruebas de los cortafuegos

UNIDAD DIDÁCTICA 9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

42. Introducción al análisis de riesgos
43. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
44. Particularidades de los distintos tipos de código malicioso
45. Principales elementos del análisis de riesgos y sus modelos de relaciones
46. Metodologías cualitativas y cuantitativas de análisis de riesgos
47. Identificación de los activos involucrados en el análisis de riesgos y su valoración

48. Identificación de las amenazas que pueden afectar a los activos identificados previamente
49. 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
50. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
51. 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
52. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
53. Determinación de la probabilidad e impacto de materialización de los escenarios
54. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
55. 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
56. Relación de las distintas alternativas de gestión de riesgos
57. Guía para la elaboración del plan de gestión de riesgos
58. Exposición de la metodología NIST SP 800-30
59. Exposición de la metodología Magerit versión 2

UNIDAD DIDÁCTICA 10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

60. Herramientas del sistema operativo tipo Ping, Traceroute, etc.
61. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
62. Herramientas de análisis de vulnerabilidades tipo Nessus

63. Analizadores de protocolos tipo WireShark, DSniff, Cain Abel, etc.
64. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
65. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

UNIDAD DIDÁCTICA 11. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

66. Principios generales de cortafuegos
67. Componentes de un cortafuegos de red
68. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
69. Arquitecturas de cortafuegos de red
70. Otras arquitecturas de cortafuegos de red

UNIDAD DIDÁCTICA 12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

71. Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
72. Guía para la elaboración del plan de auditoría
73. Guía para las pruebas de auditoría
74. Guía para la elaboración del informe de auditoría

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 del año.

http://cursosonline.workingformacion.com

DURACIÓN

200 horas

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