ACADEMIA INTEGRAL
CENTRO DE NUEVAS TECNOLOGIAS

LA FORMACIÓN ES LA CLAVE DEL ÉXITO

Guía del Curso

COMM03 Gestión de la ciberseguridad en PYMES. Comercio Electrónico Seguro

---

Modalidad de realización del curso: A distancia y Online

Titulación: Diploma acreditativo con las horas del curso

OBJETIVOS

Este curso COMM03 Gestión de la ciberseguridad en PYMES. Comercio Electrónico Seguro ofrece una especialidad formativa de la Familia Profesional del Comercio y Marketing. Este curso COMM03 Gestión de la ciberseguridad en PYMES. Comercio Electrónico Seguro permite al alumno conocer todos aquellos aspectos en los que se basa la ciberseguridad y que pueden emplearse en PYMES para permitir aumentar la protección de nuestra seguridad e impedir ciberataques.

CONTENIDOS

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA CIBERSEGURIDAD

1. Identificación de los conceptos básicos de ciberseguridad y su relación con la seguridad
2. - Definición y alcance de la ciberseguridad
3. - Áreas de actuación de la ciberseguridad
4. - Ubicación de la ciberseguridad
5. - Dimensiones de la seguridad y garantías que ofrece
6. - Implementación de las dimensiones
7. - Protección de la información

8. Relación entre las amenazas y las vulnerabilidades reconociendo sus efectos en los sistemas
9. - Ingeniería social
10. - Vulnerabilidades en la autenticación
11. - Malware y botnets
12. - Seguridad en el perímetro de las redes
13. - Riesgos de seguridad
14. - Incidentes de seguridad
15. Identificación de los mecanismos de defensa a implementar en las redes privadas
16. - Defensa en profundidad y la DMZ
17. - Antimalware
18. - Contraseñas
19. - Control de acceso
20. - Controles para definir una red segura
21. - Sistemas de detección de ataques
22. - Recuperación de los sistemas ante un ciberataque
23. Utilidad de la correlación de eventos en la prevención e investigación de incidentes
24. - Eventos y tipos
25. - Eventos de los sistemas de seguridad
26. - Criticidad de los eventos
27. - Tratamiento de los eventos para su automatización
28. - Soluciones de automatización. El SIEM
29. Identificación de las medidas de seguridad en las redes inalámbricas y dispositivos móviles
30. - La conexión inalámbrica y las redes
31. - Configuración de seguridad de las WLAN
32. - Medidas de seguridad en el router
33. - Amenazas en los terminales móviles
34. Caracterización de los mecanismos de protección de la información
35. - Fuga de la información
36. - Gestión de la fuga de información
37. - Métodos de copia de seguridad
38. - Restauración de los datos
39. Reconocimiento de los sistemas biométricos y aplicaciones

40. - Técnicas biométricas
41. - Aplicaciones de la biometría
42. - Gestión de riesgos en biometría
43. Identificación de los servicios que se implementan en la nube
44. - Cloud computing
45. - Seguridad en la nube
46. - Servicios de seguridad en la nube
47. Caracterización de los diferentes tipos de ciberataques
48. - Categorías de los ciberataques
49. - Ataques para obtener información
50. - Ataques a nivel de red
51. - Ataques de monitorización
52. - Ataques de autenticación
53. - Ataques de denegación de servicio

UNIDAD DIDÁCTICA 2. APLICACIÓN DE LA CIBERSEGURIDAD EN LAS PYMES

1. Introducción de la ciberseguridad en la empresa
2. - Seguridad en la empresa
3. - Causas de los ataques en la empresa
4. - Revisión de ciberseguridad en la empresa
5. - Pilares de una estrategia de ciberseguridad
6. - Roles en ciberseguridad
7. - Controles de seguridad a establecer en una organización
8. Identificación del usuario como elemento de ciberseguridad en la empresa
9. - Rol del usuario en el puesto de trabajo
10. - Protección del puesto de trabajo
11. - Acceso remoto y teletrabajo
12. - Escritorio virtual
13. Detección de necesidades de protección y seguridad en las empresas
14. - Clasificación de la información empresarial
15. - Medidas de protección de la información
16. - Almacenamiento seguro de la información

17. - Eliminación de los datos. Borrado seguro
18. - Conservación de la información
19. - Almacenamiento extraíble
20. Desarrollo de planes y políticas de seguridad en una empresa
21. - Plan director de seguridad
22. - Políticas de seguridad dirigidas a los componentes de la empresa
23. - Normas y procedimientos técnicos
24. Utilidad de los planes de continuidad de negocio en la empresa
25. - Análisis y gestión de riesgos
26. - Plan de continuidad de negocio
27. - Plan de contingencia
28. - Auditorías de seguridad
29. Necesidad de un plan de recuperación de desastres en la empresa
30. - En plan de recuperación de desastres
31. - Guía de desarrollo de un plan de recuperación de desastres
32. Introducción a la seguridad en el comercio electrónico
33. - Identidad digital y reputación empresarial
34. - Cliente online y su protección
35. - Redes sociales y la empresa
36. - Fraude online
37. - Protección de la web
38. Aplicación de medidas de ciberseguridad en redes inalámbricas y dispositivos móviles
39. - Formas de ataque y métodos de seguridad en las redes inalámbricas
40. - Sistemas de gestión de dispositivos móviles de la empresa
41. - Estrategia BYOD
42. Caracterización de la tecnología IoT en la empresa
43. - IoT en la empresa en la actualidad y en el futuro.
44. - Riesgos de seguridad
45. - Recomendaciones de seguridad

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