

SOLUCIONES

La firma digital



IFCM012PO




Informática y
comunicaciones



20 horas de
formación

editorial **cep**



**SOLUCIONES
TEST**

Soluciones Tema 1

Firma digital

1. b) Firma digital
2. a) Criptografía
3. a) Certificado de persona física
4. d) Representante para administrador solidario
5. a) Certificado hardware
6. c) Certificado de sello electrónico
7. b) Prestador de servicios de certificación
8. d) 2003
9. c) Que no se puede decir que no se ha firmado un documento
10. a) eIDAS

Soluciones Tema 2

Contenido y alcance

1. c) Sociedad de la información
2. c) Fritz Machlup
3. d) Heterogeneidad de los códigos para convertir diversos tipos de información
4. c) La automatización de tareas
5. c) Brecha tecnológica
6. c) Diferencia tecnológica
7. b) Territoriales
8. a) 4.500 millones
9. d) 2018
10. b) Biotecnología

Soluciones Tema 3

Normativa reguladora

1. a) 2007
2. c) 1999
3. d) LSSI
4. b) Seguridad jurídica
5. b) Límite de la libertad de expresión
6. c) Tecnología social
7. c) Disponibilidad horaria
8. c) C2B
9. a) B2C
10. a) 40 %

Soluciones Tema 4

Solicitud y obtención

1. b) Seguridad tecnológica
2. b) Fábrica Nacional de Moneda y Timbre
3. d) Soporte técnico
4. d) Certificados raíz
5. d) Certificados “timestamping” cualificado
6. b) Solicitar el certificado
7. b) Privacidad y seguridad
8. c) Importar
9. a) Exportar
10. a) Protocolo OCSP

Soluciones Tema 5

Seguridad y recomendaciones

1. c) Seguridad informática
2. b) Agencia Española de Protección de Datos
3. a) Programa informático malicioso
4. c) Antivirus identificadores
5. d) Phishing
6. d) Spoofing
7. b) Son archivos que simulan ser normales para infectar al equipo
8. c) Un protocolo de seguridad
9. d) Seguridad física informática
10. b) Incendios

Soluciones Tema 6

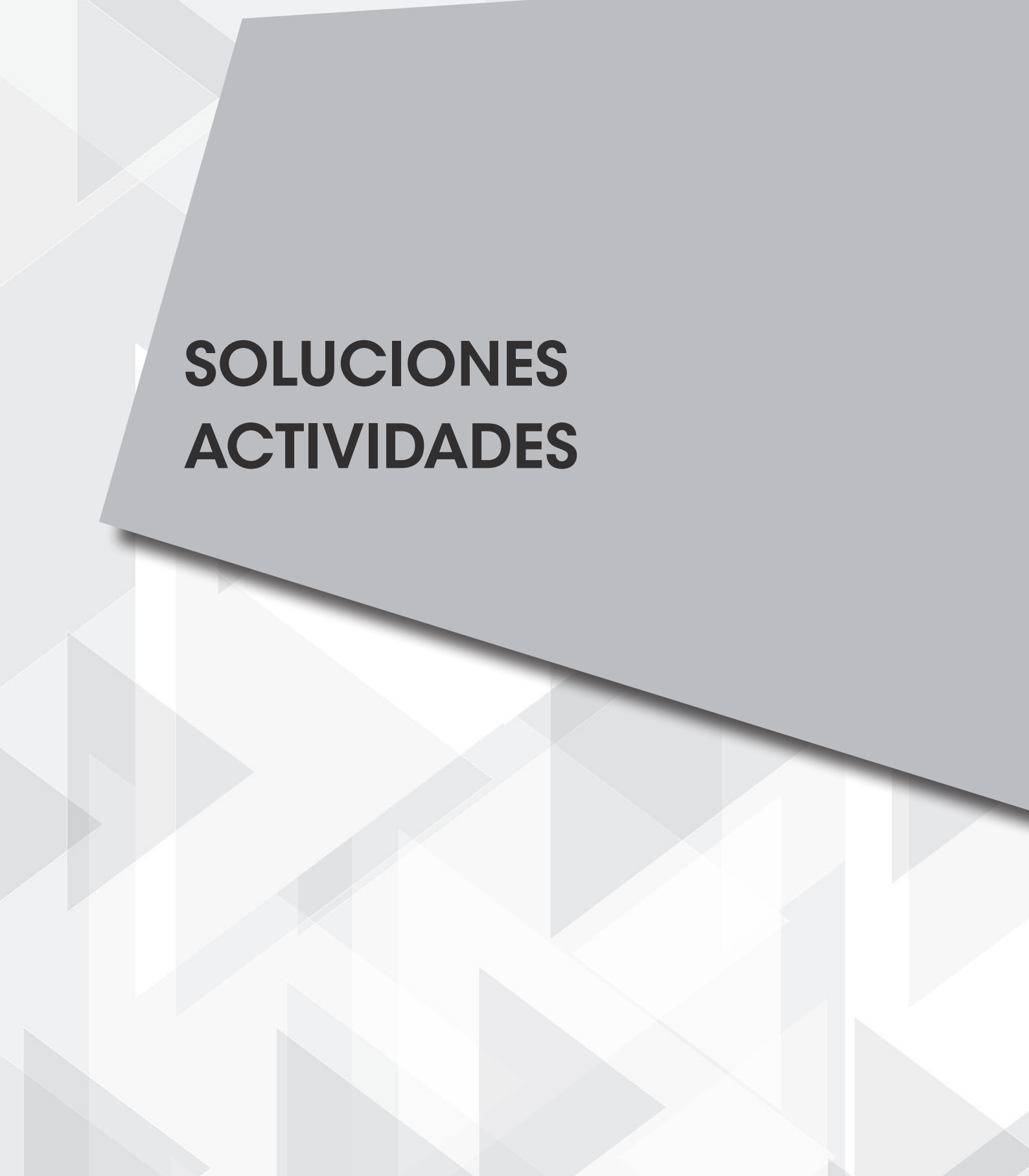
Uso de la firma digital

1. d) Firma manuscrita
2. a) Administración central
3. b) Transacción financiera
4. c) Aumento de costes de envíos postales
5. c) Banca on-line
6. b) Facua
7. c) 2015
8. d) AEAT
9. d) Encriptación
10. b) Outlook

Soluciones Tema 7

Necesidad de sistemas de seguridad en la empresa

1. a) Integridad
2. d) Cuerpo Nacional de Policía
3. b) Fallos no corregidos de los fabricantes
4. c) Backdoors
5. b) Seguridad electrónica
6. c) Protección de claves
7. b) Central receptora
8. d) Cámara
9. d) Detector de metales
10. c) Estación repetidora



**SOLUCIONES
ACTIVIDADES**

Soluciones Tema 1

Firma digital

1.

| | |
|---------------------|---|
| Primer paso | El usuario dispone de un documento electrónico, como un pdf o una imagen, y un certificado electrónico que le pertenece y lo identifica. |
| Segundo paso | La aplicación utilizada para la firma realiza un resumen del documento. Se trata de un resumen de unas líneas que es único, cuya modificación implica también una modificación del resumen. |
| Tercer paso | La aplicación utiliza la clave privada para codificar el resumen. |
| Cuarto paso | La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este documento es la firma electrónica. |

2.

| | |
|---------------------------------------|--|
| Firma electrónica indirecta | Se trata de la identificación y verificación de identidad de una persona mediante un nombre de usuario y contraseña. |
| Firma electrónica en e-mails | Consiste en el envío de un e-mail firmado en el que se adjuntan uno o más documentos. |
| Firma electrónica en documento | Consiste en el envío de documentos electrónicos que tienen la firma dentro de su estructura. |

3.

- b) Permitir la identificación del firmante
- c) Haber sido creada utilizando datos de creación de la firma electrónica
- d) Estar vinculada con los datos firmados

4.

- a) Que sea una firma electrónica avanzada
- c) Que esté basada en un certificado reconocido
- d) Que sea generada mediante un dispositivo seguro de creación de firma

Soluciones Tema 2

Contenido y alcance

1.

| | |
|-----------------------|--|
| Inmaterialidad | Podemos almacenar y acceder a información inmaterial ubicada en cualquier lugar. |
| Interactividad | Permiten la comunicación bidireccional entre los usuarios. |
| Digitalización | Es la transformación de la información analógica en códigos numéricos. |
| Colaboración | Permiten el trabajo en equipo. |

2.

| | |
|-----------------------------------|--|
| Sociedad industrial | Se accede a los bienes producidos por otro. |
| Sociedad posindustrial | Se accede a los servicios prestados por otros. |
| Sociedad de la información | Se accede a los datos generados por otros. |

3.

- a) Globalización
- b) Tecnología
- d) El rápido funcionamiento de todas las actividades de la vida social

4.

| | |
|------------------|--|
| Economía | Facilita el trabajo en las empresas debido a la mejoras para almacenar, procesar y difundir la información. |
| Política | Mejora de las campañas electorales con el uso de internet, los plenos o las votaciones. |
| Salud | Creación de la telemedicina, que permite la consulta por internet, el seguimiento del paciente, etc. |
| Educación | Mejora la calidad educativa gracias al uso de internet, proyectores, videoconferencias, libros digitales, etc. |

5.

| | |
|-----------------------|--|
| Deportes | Uso de nuevos dispositivos tecnológicos como los pulsómetros, velocímetros o GPS. |
| Vida | Mejora de las actividades sociales en avances en términos de telefonía móvil, música, juegos, etc. |
| Guerra | Creación de armamento como bombas atómicas o misiles. |
| Administración | Mejora de los trámites administrativos. |

6.

- a) Redes sensoriales
- c) Detectores de incendios

Soluciones Tema 3

Normativa reguladora

1.

| | |
|-------------------------|--|
| Catálogo virtual | Los clientes pueden ver el catálogo de productos o servicios a través de internet, además de otras acciones, como hacer pedidos y pagos on-line. |
| Ubicuidad | Permite realizar las compras desde cualquier lugar y a cualquier hora. |
| Alcance global | El mercado es global, ya que cualquier persona conectada a la red puede comprar por internet. |
| Espacio virtual | Tener una plataforma de comercio electrónico supone un ahorro de espacio debido a que no se necesita un espacio físico para mostrar los productos. |

2.

| | |
|-----------------------------------|--|
| Virtualidad | La interacción con el cliente solo se realiza de manera on-line. |
| Interacción | La comunicación con los clientes no se produce de forma presencial, sino a través de herramientas tic como el correo electrónico, el chat o el teléfono. |
| Personalización | Poseer una plataforma de venta on-line permite usar mecanismos de marketing más personalizados. |
| Densidad de la información | La información que se ofrece es mucho mayor que a través de métodos tradicionales. |

3.

| | |
|------------------------------------|--|
| B2B: Business to Business | Es el comercio entre empresas. |
| B2C: Business to Consumer | Son las tiendas virtuales destinadas a consumidores. |
| C2C: Consumer to Consumer | Son las transacciones entre consumidores. |
| G2C: Government to Consumer | Son los trámites administrativos gubernamentales que incluyen una transacción por tasas. |

4.

- a) Confiar en e-mails con grandes ofertas
- c) No usar el modo de navegación privada

5.

| | |
|--|---|
| Obligaciones de las empresas | Toda empresa de comercio electrónico está obligada a informar a los usuarios acerca de todos los trámites que se seguirán en el proceso de la compras de los productos o contratación de los servicios. |
| Envío de comunicaciones comerciales | No se podrá, sin consentimiento expreso del consumidor, enviar comunicaciones comerciales de publicidad, promociones o de cualquier otro tipo. |
| Protección de datos | Se debe garantizar la protección de los datos personales. Para este fin el consumidor deberá dar su consentimiento para la recolección de estos datos. |
| Aviso legal | Se deben mostrar en la página web los datos de la empresa. Algunos de estos datos son: nombre, domicilio social, dirección de correo electrónico, número de identificación fiscal, etc. |

Soluciones Tema 4

Solicitud y obtención

1.

| | |
|-------------------------|--|
| Integridad | Tanto de los datos, como de la fuente de los datos. |
| Disponibilidad | La información estará disponible a los usuarios que posean el permiso para acceder a ella. |
| Confidencialidad | El acceso a la información debe estar controlado. |
| Autenticación | Identificación de los usuarios. |

2.

- a) Google Chrome
- d) Mozilla Firefox

3.

| | |
|-------------------------------------|--|
| Certificados de componente | Se emite para la identificación de servidores o las aplicaciones informáticas que tengan autoridad de certificación. |
| Administración pública | Se emite para el personal de las Administraciones públicas. |
| Persona física | Se emite para los ciudadanos que estén en posesión de un DNI. |
| Certificado de representante | Se emite para un administrador único o solidario, persona jurídica o entidad sin personalidad jurídica. |

4.

- a) Se aconseja formatear el ordenador.
- c) Se deben hacer las actualizaciones oportunas.

5.

- a) Asociación Nacional de Fabricantes
- b) Policía Nacional
- d) Firma profesional

Soluciones Tema 5

Seguridad y recomendaciones

1.

| | |
|--------------------------|---|
| Mínimo privilegio | Se deben otorgar los permisos estrictamente necesarios para las acciones requeridas, ni más ni menos. |
| Eslabón más débil | El atacante siempre va a centrarse en el punto más débil del sistema. |
| Proporcionalidad | Las medidas de seguridad deben ser las adecuadas para lo que se protege y el nivel de riesgo existente. |
| Dinamismo | La seguridad informática requiere un mantenimiento constante. |

2.

| | |
|--|---|
| Virus de RAM | Se alojan en la memoria y se activan cuando el sistema operativo se ejecuta. |
| Virus de acción directa | Se encuentran en el directorio raíz del disco duro y carga ciertas operaciones con el arranque. |
| Virus de sobreescritura | Borran la información de ficheros. |
| Virus de secuencias de comandos web | Infectan el código de contenido de varias web. |

3.

| | |
|--------------------------|--|
| Macrovirus | Infectan archivos que se crean con ciertas aplicaciones o programas. |
| Virus polimórfico | Se encriptan utilizando diferentes claves. |
| Virus fat | Impiden el acceso a secciones del disco duro con archivos importantes. |
| Virus de boot | Imposibilita el arranque del dispositivo. |

4.

| | |
|----------------------------|--|
| Phishing redirector | Se realiza mediante la copia de dos sitios web de confianza desde donde se roban las credenciales. |
| Spear phishing | Está dirigido a personas o grupos reducidos. Al ser personalizada, a veces la estafa es mayor. |
| Smishing | Es el phishing a través de SMS. Suele servir para obtener dinero. |
| Pharming | Consiste en modificar el sistema de dominios DNS para conducir al usuario a una página web falsa. |

5.

| | |
|-------------------|---|
| Spyware | Son programas espías que recopilan información del usuario sin su consentimiento. No daña al ordenador, pero atenta contra la privacidad del usuario. |
| Adware | Es un programa malicioso que se instala en el ordenador y cuya función es descargar y mostrar anuncios publicitarios como ventanas emergentes. |
| Ransomware | Secuestra los datos de un ordenador y pide un rescate económico a cambio de liberarlo. |
| Spam | Es el correo basura. Se envía de forma masiva para propagar códigos maliciosos. |

Soluciones Tema 6

Uso de la firma digital

1.

| | |
|---------------------------|--------------------------------|
| Administración central | Loterías y Apuestas del Estado |
| Administración autonómica | Junta de Andalucía |
| Administración local | Ayuntamiento de Granada |
| Otros organismos | Correos y Telégrafos |

2.

| | |
|------------------------|-------------------------------------|
| Ministerio de Justicia | Consultar antecedentes penales |
| Seguridad Social | Gestionar datos de autónomo |
| Ayuntamientos | Certificado de empadronamiento |
| Agencia Tributaria | Realizar la declaración de la renta |

3.

- a) Consultar edad de jubilación
- b) Trámites del sistema sanitario

4.

| | |
|------------------------------------|---|
| Autoridad certificatoria | Incluye el marco para proveer los servicios necesarios para generar el certificado y la firma electrónica. |
| Propietarios de páginas web | Desde gobiernos y universidades hasta negocios o ciudadanos individuales son los que deben decidir el nivel de seguridad de sus sitios web. |
| Navegadores web | Determinan la confianza en los proveedores del certificado, ya que los más usados usan una guía para determinar el nivel de seguridad. |
| Usuarios finales | Incluye tanto las personas físicas como las entidades legales que acceden a un sitio web que contiene un certificado de autenticación web. |

5.

- a) Symantec
- b) Comodo
- d) GlobalSign

Soluciones Tema 7

Necesidad de sistemas de seguridad en la empresa

1.

| | |
|-------------------------|--|
| Confidencialidad | El sistema de seguridad va a manejar información secreta y de acceso restringido, permitiendo reconocer intrusiones y enviar información remota con protección. |
| Disponibilidad | Se basa en el tiempo que un dispositivo, aparato o sistema está en disponibilidad de uso, el tiempo de funcionamiento o el tiempo total de conexión del sistema. |
| Confiabilidad | Es la capacidad de un producto o servicio de cumplir con la función para la que está diseñado. |
| Autenticación | Es tanto el ingreso-salida del personal desde y hacia un lugar restringido como los registros de acceso de los dispositivos electrónicos que permiten obtener información a usuarios restringidos. |

2.

| | |
|-----------------------------|---|
| Medios humanos | Son aquellos medios o recursos constituidos por personal capacitado de seguridad pública o privada. |
| Medios técnicos | Son los recursos físicos encaminados a mantener la seguridad de sitios y personas. |
| Medios organizativos | Son las herramientas usadas en la organización y coordinación en el uso de recursos, como la planificación, asignación de recursos, normas de seguridad, etc. |

3.

| | |
|--|---|
| Factores de diseño | Debilidad en el diseño de protocolos utilizados en las redes. |
| Factores de implementación | Errores de programación no depurados. |
| Factores de uso | Configuración incorrecta de los sistemas informáticos. |
| Factores de vulnerabilidades del día cero | Son aquellas vulnerabilidades conocidas para las cuales aún no se han creado parches, revisiones o actualizaciones y que se emplean para llevar a cabo un ataque. |

4.

| | |
|---|---|
| Bloquear la sala de servidores | Deben instalarse cerraduras en la sala y establecer una política de ingreso en la misma. |
| Configurar la vigilancia | Instalar un sistema de autenticación o cámaras de vigilancia. |
| Cuidar las estaciones de trabajo | Deben desconectarse los ordenadores que no estén en uso. |
| Deshabilitar unidades | Hay que desactivar o eliminar unidades de disquete, puertos USB y otros medios de conectar unidades externas. |

5.

| | |
|----------------------------------|---|
| Unidad central de control | Es el elemento que recibe las señales eléctricas de los sensores y que, a su vez, permite que se envíen las señales a una central. Es lo que se conoce como centralita. |
| Sensores o detectores | Son los dispositivos que perciben lo que ocurre en el lugar que se está protegiendo. Pueden ser sensores de movimiento, sensores de humo, etc. |
| Interfaz de usuario | Es el elemento que permite a un ser humano controlar e interactuar con una máquina o sistema, es decir, el elemento que sirve para manejar el sistema de seguridad. |
| Red de conexión | Es el elemento que sirve para conectar todos los dispositivos del sistema de seguridad entre sí. |