Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. **El conjunto de datos digitales que son utilizados con el objetivo de identificar a un firmante es:**

    a. Firma.
    b. Firma electrónica.
    c. Firma digital.
    d. Certificado digital.

2. **El conjunto de caracteres que se añade al final de un documento o mensaje para informar, dar validez y seguridad al mismo es:**

    a. Firma.
    b. Firma electrónica.
    c. Firma digital.
    d. Certificado digital.

3. **El documento, fichero o archivo informático que se usa para identificarse en la red, está autentificado por terceros de confianza y contiene la firma digital es:**

    a. Firma.
    b. Certificado digital.
    c. Firma digital.
    d. Firma electrónica.

4. **Indica cuál de las siguientes no es una función de la firma electrónica:**

    a. Permitir la identificación del firmante inequívocamente.
    b. Asegurar la integridad del certificado electrónico y sus documentos adjuntos.
    c. Asegurar la integridad del documento firmado.
    d. Asegurar la integridad de la firma.

5. Indica cuál de los siguientes no es un requisito en los que se basa la firma electrónica:

a. Identificar al firmante.
b. Verificar la integridad del documento firmado.
c. Contar con la participación de terceros de confianza.
d. Garantizar el repudio en origen.

6. El artículo 3.3 de la Ley 59/2003, de 19 de diciembre, recoge esta definición: "firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma". ¿A qué concepto hace referencia?

a. Firma electrónica reconocida.
b. Certificado de seguridad.
c. Rúbrica digital.
d. Firma digital unificada.

7. La firma digital incluye:

a. Solamente datos.
b. Nombre y DNI.
c. Mecanismos de encriptación.
d. No incluye nada, es solo la rúbrica que se muestra visualmente.

8. Señala cuál de las siguientes es una propiedad de la firma digital:

a. Verificable.
b. Infalsificable.
c. Innegable.
d. Todas las opciones son correctas.

9. Los tipos de firma digitales son:

a. Básica, avanzada y reconocida.
b. Simple, media y reconocida.
c. Simple, básica y reconocida.
d. Simple, avanzada y reconocida.

10. ¿De qué forma puede obtenerse un certificado digital?

a. Por medio de un archivo informático.
b. Por medio de un archivo para *Android*.
c. Mediante un DNIe.
d. Todas las opciones son correctas.

Ejercicios de autoevaluación
Unidad de Aprendizaje 2

1. "Garantizar digitalmente la identidad de la persona que firma electrónicamente un documento en internet" es el objetivo de:

a. La firma.
b. La firma digital.
c. La firma electrónica.
d. El certificado digital.

2. El coste económico de un certificado digital...

a. ... es invariable.
b. ... varía en función del tipo de certificado a obtener.
c. ... depende de la cantidad de usos que se hagan del certificado.
d. ... depende del tipo de certificado y uso que se le dé.

3. Los certificados para la firma de código, ¿en función de qué criterio se clasifican?

a. Según las comprobaciones a realizar.
b. Según su finalidad.
c. Según quién los utiliza.
d. Según la forma del certificado.

4. SSL ofrece mecanismos:

a. De aislamiento y seguridad.
b. Solo de seguridad.
c. Solo de aislamiento.
d. Todas las opciones son incorrectas.

5. Un certificado SSL consta de dos partes:

a. Llave pública y llave privada.
b. Llave privada y licencia pública.

c. Parte pública y parte privada.
d. Parte pública y llave pública.

6. ¿Cuál de las siguientes no es una propiedad aportada por el Certificado canalizador?

a. Incremento del tráfico.
b. Velocidad de respuesta.
c. Dar servicio a los usuarios.
d. Filtro.

7. Señala cuál de los siguientes no es un protocolo seguro en el certificado de correo electrónico:

a. SMTPS
b. POP3
c. IMAPS
d. POP3S

8. En un certificado de validación de páginas web, ¿qué color adopta la barra del navegador?

a. Puede adoptar un solo color: blanco.
b. Puede adoptar dos colores: rojo y verde.
c. Puede adoptar tres colores: rojo, verde y blanco.
d. La barra del navegador no adopta color alguno.

9. Los certificados de sello se basan en un certificado digital que incluye:

a. Número de identificación fiscal.
b. Denominación de la Administración.
c. Identidad de la persona titular.
d. Todas las opciones son correctas.

10. Señala cuál de los siguientes no es un objetivo de los certificados de fecha y hora:

a. Aumentar la confianza del comercio electrónico.
b. Atraer más visitantes al sitio web.
c. Protección de identidad intelectual.
d. Ampliación de las funcionalidades de la firma electrónica.

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. **Las medidas de seguridad se centran en:**

   a. *Hardware* y *software*.
   b. Redes.
   c. *Hardware, software* y redes.
   d. Todas las opciones son incorrectas.

2. **El tipo de seguridad que en informática se destina a prevenir cualquier tipo de ataque en un entorno o sistema informático es:**

   a. Seguridad activa.
   b. Seguridad pasiva.
   c. Seguridad física.
   d. Seguridad lógica.

3. **El tipo de seguridad que en informática se centra en la minimización de los daños causados por un usuario, por un accidente o por algún tipo de riesgo o amenaza informática es:**

   a. Seguridad activa.
   b. Seguridad pasiva.
   c. Seguridad física.
   d. Seguridad lógica.

4. **Indica cuál de las siguientes no es una desventaja de la seguridad activa:**

   a. Mantenimiento
   b. Coste
   c. Personal
   d. Contraseñas

5. Indica cuál de las siguientes no es una desventaja de la seguridad pasiva:

a. Coste
b. Almacenamiento
c. Actualizaciones
d. Contraseñas

6. Indica cuál de las siguientes no es una técnica de la seguridad pasiva:

a. Usar *hardware especializado.*
b. Antivirus.
c. Usuarios auxiliares.
d. Desconexiones.

7. Indica cuál de las siguientes no es una técnica de la seguridad activa:

a. Contraseñas seguras.
b. Escaneos completos.
c. Antivirus.
d. Encriptación.

8. El conjunto de técnicas mediante las cuales los atacantes (ciberdelincuentes) se hacen pasar por una determinada entidad o empresa a través de la falsificación o engaño en sus datos de comunicación se conoce como:

a. Seguridad activa.
b. *Phising.*
c. *Spoofing.*
d. Seguridad pasiva.

9. Indica cuál de las siguientes no es una técnica de suplantación de identidad:

a. Suplantación de *firewall.*
b. Suplantación de IP.
c. Suplantación de correo electrónico.
d. Suplantación de web.

10. Indica cuál de los siguientes protocolos no es seguro:

a. HTTP
b. HTTPS
c. SET
d. SSL