Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La autenticación digital es un proceso que consiste únicamente en declarar la propia identidad ante un sistema informático, sin necesidad de probarla.

- Verdadero
- **Falso**

b. El Reglamento eIDAS establece tres niveles de firma electrónica: simple, avanzada y cualificada.

- **Verdadero**
- Falso

c. El certificado electrónico de ciudadano emitido por la FNMT-RCM tiene una validez de 10 años.

- Verdadero
- **Falso**

d. Para renovar telemáticamente el certificado electrónico, es necesario volver a acreditar la identidad de forma presencial.

- Verdadero
- **Falso**

e. La firma electrónica cualificada tiene la misma eficacia jurídica que la firma manuscrita en todos los casos.

- **Verdadero**
- Falso

2. ¿Cuál de las siguientes afirmaciones describe correctamente la diferencia entre la firma electrónica y la firma digital?

a. Son términos completamente sinónimos que se pueden usar indistintamente en cualquier contexto.
b. La firma digital es el concepto jurídico y la firma electrónica es la implementación tecnológica que la hace posible.
c. La firma electrónica es el concepto jurídico y funcional; la firma digital es la implementación tecnológica basada en criptografía que la hace posible.
d. La firma digital solo puede usarla la Administración pública; la firma electrónica puede usarla cualquier ciudadano.

3. ¿Qué es el Reglamento eIDAS?

a. Una norma española que regula exclusivamente el DNI electrónico.
b. Una directiva europea de obligado cumplimiento solo para las administraciones públicas.
c. Un reglamento de la Unión Europea de aplicación directa en todos los Estados miembros que regula la identificación electrónica y los servicios de confianza.
d. Una norma técnica de estandarización de los algoritmos de cifrado.

4. ¿Qué función cumple la clave privada en el proceso de firma electrónica?

a. Se usa para descifrar los mensajes recibidos y debe publicarse para que cualquiera pueda verificar la identidad del titular.
b. Se usa para firmar documentos y debe mantenerse en secreto bajo la custodia exclusiva de su propietario.
c. Se usa para acceder a las sedes electrónicas de las administraciones públicas y debe cambiarse cada tres meses.
d. Se usa para cifrar el contenido del certificado electrónico y es administrada por la FNMT-RCM.

5. ¿Cuál es la principal diferencia entre el DNIe y el DNIe 3.0?

a. El DNIe 3.0 es el único que incorpora el certificado de autenticación; el DNIe anterior solo incorpora el certificado de firma.
b. El DNIe 3.0 no requiere PIN de seguridad para su uso, mientras que el DNIe original sí lo requiere.
c. El DNIe 3.0 incorpora tecnología NFC que permite usarlo con *smartphones* sin necesidad de lector de tarjetas; los DNIe anteriores no tienen esta tecnología.
d. El DNIe 3.0 es el único que tiene validez jurídica como documento de identificación presencial.

6. ¿En qué orden deben realizarse las fases del proceso de obtención del certificado electrónico de ciudadano de la FNMT-RCM?

a. Solicitud *online* → Descarga del certificado → Acreditación de identidad → Configuración del navegador.
b. Acreditación de identidad → Configuración del navegador → Solicitud *online* → Descarga del certificado.
c. Configuración del navegador → Solicitud *online* → Acreditación de identidad → Descarga del certificado.
d. Descarga del certificado → Configuración del navegador → Acreditación de identidad → Solicitud *online.*

7. ¿Qué ocurre si el certificado electrónico ya ha caducado cuando el titular intenta renovarlo?

a. Puede renovarlo igualmente de forma telemática, ya que la FNMT-RCM mantiene el certificado activo durante 30 días después de su caducidad.
b. Solo puede renovarlo si acude presencialmente a una oficina de la Agencia Tributaria.
c. Debe iniciar el proceso de obtención desde cero, incluyendo la acreditación presencial de su identidad, ya que el certificado caducado no puede utilizarse para la renovación telemática.
d. El certificado se renueva automáticamente en el momento de la caducidad si el equipo está conectado a internet.

8. Relaciona cada herramienta con su función principal:

a. AutoFirma
b. VALIDe
c. Cl@ve PIN
d. CERES (www.cert.fnmt.es)

c. Plataforma de identificación *online* mediante código de un solo uso enviado al móvil.
a. Aplicación oficial para firmar documentos electrónicamente con el certificado instalado en el equipo.
d. Sede electrónica de la FNMT desde donde se solicita, descarga y gestiona el certificado de ciudadano.
b. Servicio oficial de verificación de la autenticidad de firmas y certificados electrónicos.

9. ¿Cuál de las siguientes modalidades de acreditación de identidad para obtener el certificado electrónico tiene algún coste económico?

a. La acreditación presencial en una oficina de la Agencia Tributaria.
b. La videoidentificación mediante videollamada con un agente de registro.
c. La acreditación con el DNIe de forma telemática.
d. La acreditación presencial en una comisaría de policía.

10. ¿Cuál de las siguientes acciones es la más recomendable desde el punto de vista de la eficiencia energética en el uso de medios electrónicos?

a. Imprimir todos los documentos electrónicos para tener una copia física de seguridad.
b. Mantener el ordenador encendido 24 horas al día para no interrumpir la sincronización de archivos en la nube.
c. Renovar el equipo informático cada año para disponer siempre del modelo con mayor rendimiento.
d. Configurar el modo de ahorro de energía en todos los dispositivos, apagar los equipos cuando no se usen y optar por proveedores de servicios digitales que utilicen energías renovables.

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. El Reglamento (UE) n.° 910/2014 (eIDAS), modificado por el Reglamento (UE) 2024/1183 (eIDAS 2), es una directiva europea que debe ser transpuesta por cada Estado miembro, por lo que su aplicación varía en función de la legislación nacional.

- Verdadero
- **Falso**

b. La firma electrónica cualificada tiene la misma eficacia jurídica que la firma manuscrita en todos los casos y no puede ser rechazada en ningún procedimiento judicial de la Unión Europea.

- **Verdadero**
- Falso

c. La función *hash* puede revertirse para obtener el documento original a partir del resumen.

- Verdadero
- **Falso**

d. Ante la sospecha de que un certificado electrónico ha sido comprometido, lo primero que debe hacer el titular es solicitar un nuevo certificado y esperar a que el anterior caduque de forma natural.

- Verdadero
- **Falso**

e. Los algoritmos SHA-1 y MD5 están considerados seguros para el uso en firmas electrónicas modernas.

- Verdadero
- **Falso**

2. ¿Cuál es la principal diferencia entre la Directiva 1999/93/CE y el Reglamento (UE) n.° 910/2014 (eIDAS), modificado por el Reglamento (UE) 2024/1183 (eIDAS 2), en cuanto a su aplicación en los Estados miembros?

a. La Directiva 1999/93/CE es de aplicación directa y uniforme en todos los Estados miembros; el Reglamento (UE) n.° 910/2014 (eIDAS), modificado por el Reglamento (UE) 2024/1183 (eIDAS 2), requiere transposición nacional.
b. El Reglamento (UE) n.° 910/2014 (eIDAS), modificado por el Reglamento (UE) 2024/1183 (eIDAS 2), es de aplicación directa y uniforme en todos los Estados miembros; la Directiva 1999/93/CE requería transposición nacional, lo que generaba fragmentación entre los ordenamientos.
c. Ambos son directivas y requieren transposición; la diferencia es que el Reglamento (UE) n.° 910/2014 (eIDAS), modificado por el Reglamento (UE) 2024/1183 (eIDAS 2), permite más margen de adaptación nacional.
d. No existe diferencia significativa: ambos instrumentos establecen los mismos requisitos con igual nivel de aplicación.

3. ¿Qué propiedad de la función *hash* permite detectar que un documento ha sido modificado después de ser firmado electrónicamente?

a. Su carácter unidireccional: a partir del *hash* no puede reconstruirse el documento original.
b. Su resistencia a colisiones y su sensibilidad a cualquier cambio: cualquier modificación del documento, por mínima que sea, produce un *hash* completamente diferente.
c. Su longitud fija: el *hash* tiene siempre el mismo número de caracteres, lo que impide manipularlo.
d. Su algoritmo de generación público: al ser conocido, cualquier sistema puede verificar su autenticidad.

4. ¿Cuál de los siguientes componentes de la PKI es responsable de verificar la identidad del solicitante antes de que se emita el certificado electrónico?

a. La autoridad de certificación (CA)
b. La autoridad de registro (RA)
c. El repositorio de certificados
d. El servicio OCSP

5. ¿Qué formato de archivo (.p12 / .pfx) se usa para almacenar de forma protegida el certificado electrónico y la clave privada juntos?

a. X.509.
b. XAdES.
c. PKCS#12.
d. CAdES.

6. Laura recibe un correo de "renovacion@aeat-segura.es" indicándole que debe actualizar su certificado "en las próximas 2 horas". ¿Cuál es la señal de alerta más importante y qué debe hacer?

a. La señal de alerta es el plazo de 2 horas, que es demasiado corto. Debe acceder al enlace del correo para comprobar si es real, pero usando una contraseña de un solo uso.
b. La señal de alerta es el dominio del remitente: "aeat-segura.es" no es un dominio oficial de la AEAT. Laura debe ignorar el correo, no hacer clic en ningún enlace y acceder directamente a la sede oficial de la AEAT escribiendo la URL en el navegador.
c. La señal de alerta es que la AEAT no gestiona certificados electrónicos. Laura debe reenviar el correo a la FNMT-RCM para que lo verifiquen.
d. No hay señales de alerta claras; podría ser un correo legítimo. Laura debe acceder al enlace con precaución y verificar su certificado.

7. ¿Cuál es la primera acción que debe tomar un titular al sospechar que su certificado electrónico ha sido comprometido?

a. Solicitar un nuevo certificado en www.cert.fnmt.es y esperar a que el comprometido caduque de forma natural.
b. Cambiar la contraseña de acceso a las sedes electrónicas donde usa el certificado.
c. Revocar inmediatamente el certificado comprometido en www.cert.fnmt.es.
d. Comunicarlo a la Agencia Tributaria para que bloquee los trámites asociados a ese certificado.

8. Relaciona cada norma con su descripción correcta:

a. Directiva 1999/93/CE
b. Ley 59/2003
c. Reglamento (UE) n.° 910/2014 (eIDAS), modificado por el Reglamento (UE) 2024/1183 (eIDAS 2)
d. Ley 6/2020

d. Norma española que complementa el Reglamento (UE) n.° 910/2014 (eIDAS), modificado por el Reglamento (UE) 2024/1183 (eIDAS 2), regulando aspectos específicos delegados a cada Estado miembro. Derogó la Ley 59/2003.
a. Primer marco jurídico europeo para la firma electrónica. Fue una directiva, lo que generó fragmentación entre los ordenamientos nacionales.
b. Ley española que transpuso la Directiva 1999/93/CE. Estuvo vigente de 2004 a 2020.
c. Reglamento europeo de aplicación directa y uniforme en todos los Estados miembros. Define los tres tipos de firma electrónica y establece el principio de no discriminación.

9. ¿Qué protocolo permite comprobar en tiempo real, sin descargar la lista completa de revocación, si un certificado concreto está vigente o ha sido revocado?

a. TLS (Transport Layer Security)
b. PKCS#12
c. OCSP *(online Certificate Status Protocol)*
d. SHA-256

10. ¿Cuál de las siguientes afirmaciones describe correctamente la diferencia de seguridad entre el uso de una contraseña y el uso de un certificado digital para autenticarse ante una sede electrónica?

a. La contraseña es más segura porque puede cambiarse en cualquier momento; el certificado es fijo hasta su caducidad.
b. No existe diferencia significativa en términos de seguridad: ambos métodos ofrecen el mismo nivel de protección si se usan correctamente.

c. El certificado digital es más inseguro porque su archivo puede ser robado; la contraseña no deja rastro físico.
d. El certificado digital es más seguro porque la clave privada nunca viaja por la red (la operación criptográfica se realiza localmente), vincula la identidad a una autoridad de certificación reconocida y es matemáticamente infalsificable con la tecnología actual.