SOLUCIONES

# Seguridad informática y firma digital

IFCM026PO

Informática y comunicaciones

**50** horas de formación

editorialcep

# SOLUCIONES TEST

# Soluciones Tema 1

## Firma electrónica, firma digital

**1.** d) Firma electrónica

**2.** b) 2003

**3.** a) Clave privada

**4.** b) eIDAS

**5.** a) Firma electrónica indirecta

**6.** d) Con la autoridad de sellado de tiempo

**7.** b) Avanzada

**8.** b) No repudio

**9.** c) Hash

**10.** b) Certificados de persona jurídica

# Soluciones Tema 2

## Tipos de certificados

**1.** a) Capa de zócalos seguro

**2.** c) Certificados intermedios

**3.** a) Certificado con validación de dominio

**4.** c) 128 bits

**5.** a) Encriptación

**6.** c) Clave pública

**7.** b) Outlook

**8.** d) 2015

**9.** d) Solicitante

**10.** c) En una autoridad de sellado de tiempo

# Soluciones Tema 3

## Sistemas de seguridad en la empresa

**1.** b) Medios técnicos

**2.** b) Protección perimetral

**3.** c) Prevención de desastres naturales

**4.** c) Central receptora de alarmas

**5.** a) Cable coaxial

**6.** c) Grado 3

**7.** d) Blue MAC Spoofing

**8.** c) Man in the middle attack

**9.** d) Software de la autoridad de certificación

**10.** b) Vishing

# SOLUCIONES ACTIVIDADES

# Soluciones Tema 1

## Firma electrónica, firma digital

**1.**

a) Banco de España

d) Dirección General del Catastro

**2.**

a) Certificado de servidor

b) Certificado de representante

d) Certificado de apoderado

**3.**

a) Memoria USB

b) Almacén de certificados

d) Disco duro

**4.**

a) Certificado de sede electrónica

c) Certificado de empleado público

**5.**

b) El código único identificativo

c) El DNI del firmante

d) El período de validez

# Soluciones Tema 2

## Tipos de certificados

**1.**

| | |
|---|---|
| Certificados de clase 1 | Son los certificados más fáciles de obtener en los que se verifica solo el nombre y la dirección de correo electrónico del titular. |
| Certificados de clase 2 | Son certificados en los que se verifican los datos de los de clase 1, y además, el DNI o permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento. |
| Certificados de clase 3 | Son certificados en los que se piden los datos de los de clase 2 y el crédito de la persona o empresa. |
| Certificados de clase 4 | Son certificados en los que, además de los datos anteriores, se verifica la posición de una empresa dentro de una organización. |

**2.**

c) Publicar los certificados no fiables

d) Proporcionar la clave pública

**3.**

| | |
|---|---|
| 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 de certificados, ya que, los más usados, utilizan una guía para determinar el nivel de seguridad. |
| Usuarios finales | Incluye tanto a las personas físicas como a las entidades legales que acceden a un sitio web que contiene un certificado de autentificación web. |

**4.**

| | |
|---|---|
| Paso 1 | Se genera un resumen digital (hash) para el documento en el ordenador del usuario. |
| Paso 2 | La TSA genera un sello de tiempo con esta huella , la fecha y hora obtenida de una fuente fiable y la firma electrónica de la TSA. |
| Paso 3 | El sello del tiempo se envía al usuario. |
| Paso 4 | La TSA mantiene un registro de los sellos emitidos para su futura verificación. |

**5.**

a) Comercio electrónico

b) Protección de la propiedad intelectual

d) Soporte de la infraestructura PKI

# Soluciones Tema 3

## Sistemas de seguridad en la empresa

**1.**

| | |
|---|---|
| Integridad | Son las medidas o cualidades relacionadas con un sistema de seguridad para protegerlo de daños accidentales, pérdidas o modificaciones, tanto en el hardware como en el software. |
| 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. |
| Autentificación | 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.**

| | |
|---|---|
| Factores de diseño | Políticas de seguridad deficientes. |
| Factores de implementación | Existencia de puertas traseras. |
| Factores de uso | Disponibilidad de herramientas que facilitan los ataques. |
| Factores de vulnerabilidad del día cero | Se emplean para llevar a cabo un ataque. |

**3.**

| | |
|---|---|
| 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. |
| Sensores o detectores | Son los dispositivos que perciben lo que ocurre en el lugar que se está protegiendo. |
| 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. |

**4.**

| | |
|---|---|
| Sensor de movimiento | Son sensores que miden la luz infrarroja radiada por los objetos que se encuentran en su campo de actuación. |
| Sensor magnético perimetral | Son un tipo de sensores que forman un circuito cerrado con un imán y un contacto que, al separarse, producen un cambio en el campo magnético, haciendo sonar la alarma. |
| Sensor inercial | Se utilizan para detectar golpes en algún tipo de objeto. |
| Sensor de rotura de cristales | Son detectores microfónicos. |

**5.**

a) Estación base

b) Estación remota

c) Estación repetidora