Test Tema 131 #1

Actualizado el 13/04/2025

1. Según la ley 10/2021, es necesario realizar un acuerdo entre empleado y empleador para teletrabajar

a) No, aunque se recomienda
b) Si, por escrito
c) Si, y debe figurar en el contrato inicial
d) Sólo en casos excepcionales

2. Señale cuál de las siguientes opciones NO está relacionada con el ámbito del software de contenedores:

a) Kubernetes
b) Bitbucket
c) Docker
d) OpenShift

3. El proceso mediante el cual un usuario se autentica una vez en el sistema de la organización y es capaz de acceder al resto de servicios se denomina:

a) Single Login On
b) Simple Login On
c) Single Sign On
d) Simple Sign On

4. El modelo de control de accesos donde es el sistema quien protege los recursos y donde todo recurso del sistema tiene una etiqueta de seguridad se denomina:

a) De acceso discrecional (DAC)
b) De acceso obligatorio (MAC)
c) Basado en roles (RBAC)
d) De confidencialidad

5. En los sistemas de gestión de identidades, el proceso de armonización de la configuración entre el gestor de identidades y los sistemas gestionados se denomina:

a) Reconfiguración
b) Sincronización
c) Reconciliación
d) Replicación

6. En Citrix Virtual Apps and Desktops, ¿cuál de las siguientes respuestas NO es un componente de una implementación típica?

a) Citrix Switch.
b) Citrix Gateway.
c) Citrix StoreFront.
d) Citrix Estudio.

7. Indique la respuesta falsa:

a) El estándar de autenticación OAuth fue creado por la OATH (Initiative for Open Authentication).
b) OAuth 2.0 no es compatible con OAuth 1.0.
c) Graph API de Facebook solo soporta OAuth 2.0.
d) Google soporta OAuth 2.0. como método recomendado de autenticación para todas sus APIs.

8. Indicar cuál de las siguientes herramientas y protocolos permite el control remoto de puestos de usuario:

a) NNTP.

b) VNC.

c) NTP.

d) FTP.

9. Señale a qué se denomina Single sign-on (SSO):

a) Es un protocolo de cifrado para autenticar al usuario.

b) Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

c) Está asociado al cifrado basado en Secure Socket Layers (SSL).

d) Permite a través del protocolo de red HTTPS identificar a los usuarios en el acceso a servicios Web.

10. ¿Cuál de las siguientes no es un beneficio de un sistema de gestión de identidades respecto de la gestión de usuarios tradicional?

a) Informes de auditoría

b) Visión global del perfil del usuario

c) Administración delegada de usuarios

d) Todas las anteriores son beneficios

11. ¿Cual de los siguientes términos no está asociado a un sistema de gestión de identidades?

a) Metadirectorio

b) SFTP

c) LDAP

d) Single Sign On

12. Cuales de los elementos enumerados a continuación se consideran necesarios en un esquema seguro de acceso remoto a la red de una organización: 1)Acceso a una plataforma de firma digital para los usuarios de la organización. 2)Mecanismos de control de acceso a la red: portales cautivos, uso del protocolo 802.1X, etc. 3)Autenticación de usuarios y autorización: asegura la identidad y autorización de un usuario mediante el uso de protocolos de autenticación. 4)Protección de la conexión e integridad del tráfico: una vez que se establece una sesión, es necesario asegurar la confidencialidad e integridad del tráfico intercambiado entre las partes mediante cifrado. La respuesta correcta, que contiene los tres elementos necesarios es:

a) 1, 2, 3.

b) 1, 2, 4.

c) 1, 3, 4.

d) 2, 3, 4.

13. ¿Cuál de estas herramientas NO está relacionada con la gestión de identidades?

a) Oracle Identity Management

b) BMC Remedy Action Request System

c) IBM Tivoli Identity Manager

d) Novell Nsure

14. ¿Cuáles de los siguientes es un estándar que permite el intercambio de datos de autenticación y autorización?:

a) XADES

b) SAML

c) BPMN

d) PADES

15. Indique la respuesta falsa:

a) OAuth (Open Authorization) es un protocolo abierto que permite autorización segura de una API de modo estándar y simple para aplicaciones de escritorio, móviles y web.

b) OAuth y OpenID son protocolos idénticos.

c) OpenID es un estándar de identificación digital descentralizado, con el que un usuario puede identificarse en una página web a través de una URL o XRI.

d) A diferencia de arquitecturas Single Sign-On, OpenID no especifica el mecanismo de autenticación.

16. El proyecto Fidelity, de gestión de identidad federado en ámbito europeo, está basado en estándares de:

a) W3C

b) IEEE

c) CEN

d) Liberty Alliance

17. De los siguientes componentes, señale cuál no pertenece a una arquitectura genérica de gestión de identidad:

a) SP (Service Provider).

b) AP (Authentication Provider).

c) IdP (Identity Provider).

d) CoT (Circle of Trust).

18. Cuál de las siguientes afirmaciones es correcta con respecto al protocolo CAS, en el ámbito de los sistemas Single-Sign-On:

a) Fue concebido en la universidad de Oxford.

b) Es un protocolo SSO para todo tipo de aplicaciones, tanto web, como de escritorio.

c) No existe el protocolo CAS, en ese ámbito.

d) CAS son las siglas de Central Authentication Service.

19. ¿Cuál de las siguientes no es una ventaja de un sistema de gestión de identidades respecto de la gestión de usuarios tradicional?

a) Proporciona un punto único de provisión de usuarios para todos los sistemas de la organización

b) Sincronización entre sistemas

c) Gestión distribuida del ciclo de vida de los usuarios

d) Unificación de contraseñas en recursos

20. Es contenido mínimo obligatorio del acuerdo de trabajo a distancia (Señale la FALSA):

a) Inventario de los medios

b) Remuneración

c) Enumeración de los gastos

d) Lugar de trabajo a distancia

21. ¿En qué disposición está regulado el teletrabajo en España?

a) RD 28/2020

b) RD 29/2021

c) Ley 10/2021

d) Ninguna de las anteriores

22. Son principios básicos del teletrabajo (Señale la FALSA):

a) Flexibilidad

b) Voluntariedad

c) igualdad de derechos

d) La dotación de equipos

23. La decisión de trabajar a distancia será reversible:

a) Sólo a peticion de la empresa

b) Sólo a peticion del trabajador

c) Sólo en casos excepcionales

d) por parte de trabajador y empresa

24. Es una característica de Kerberos:

a) Basarse en criptografía de clave asimétrica.

b) La ausencia de un servidor de autenticación o de un servidor de tickets.

c) La ausencia de una base de datos de claves.

d) Su utilización como sistema de SSO.

25. Un sistema pide a los usuarios código de usuario y clave para identificarse. Los datos de los usuarios se almacenan en la base de datos, a excepción de las claves que se guardan en un fichero encriptado del sistema, que se actualiza cuando los usuarios cambian su clave. Este sistema ha demostrado ser poco seguro. Señale la opción más segura para mejorarlo:

a) Indexar el fichero para que el acceso sea más rápido.

b) Guardar las claves encriptadas en un campo de la tabla de usuarios.

c) Dividir el fichero en varios ficheros para mejorar el acceso, guardando en un campo de la tabla de usuarios el nombre del fichero donde reside la clave de cada usuario.

d) No guardar la clave, sino su hash y comprobar si concuerda con el hash del a contraseña introducida.

26. ¿Cuál de los siguientes conceptos NO está relacionado con la gestión de identidades?

a) CupFederation.

b) WS-Federation.

c) SAML.

d) Liberty Identity Federation Framework.

27. ¿Cuál de los siguientes términos no es un tipo de SSO (Single Sign-On)?

a) Enterprise SSO

b) Web SSO

c) Kerberos

d) Novell

28. ¿Cuál de las siguientes soluciones comerciales de Escritorio Remoto se distribuye bajo licencia propietaria?

a) Vinagre

b) DameWare Mini Remote Control

c) TightVNC

d) RdesKtop

29. Se entiende por SSO:

a) Un procedimiento de autenticación que permite acceder a diversos recursos informáticos utilizando una única identificación

b) Un sistema basado en claves SSL para la gestión remota de claves simétricas

c) Un sistema de gestión y almacenamiento de claves fraccionadas con coherencia asimétrica

d) Un procedimiento de comunicaciones seguras entre objetos basado en sockets

30. ¿Cuál de las siguientes técnicas NO se usa para encapsulado de datos en túneles VPN?

a) GRE

b) PPTH

c) IPSec

d) L2TP

31. Es una implementación de SAML:

a) OpenSAML

b) SimpleSAMLPHP

c) Shibboleth

d) Todas las anteriores

32. Indique de las siguientes opciones cuál es un estándar de federación abierta que permite a un proveedor de identidad (IdP) autenticar usuarios y, a continuación, transferir un token de autenticación a otra aplicación conocida como proveedor de servicios (SP):

a) SAML

b) JWT

c) OID

d) FIDO

33. En plataformas MDM que gestionan dispositivos Android Enterprise, ¿cómo se denominan aquellos que son propiedad de la empresa, con un uso estrictamente profesional?

a) COPE

b) BYOD

c) COBO

d) KNOX

34. Indique la opción falsa:

a) Las siglas HOTP hacen referencia al algoritmo HMAC-based One Time Password.

b) HOTP es un estándar abierto.

c) Son implementaciones de HOTP: Barada, Google Authenticator, LinOTP.

d) HOTP no puede ser utilizado para autenticar a un usuario en un sistema a través de un servidor de autenticación.

35. ¿Qué es una VPN?

a) Una red privada virtual que permite securizar mediante cifrado las comunicaciones a través de un canal.

b) Un protocolo de virtualización de aplicaciones y escritorio.

c) Una herramienta de acceso remoto a escritorios Microsoft y Linux.

d) Un sistema de virtualización de servidores físicos.

36. Indique la respuesta correcta en relación con Kerberos:

a) Se utiliza como sistema de Single Sign-On (SSO).

b) Se basa en criptografía de clave asimétrica.

c) No requiere de un servidor de autenticación ni de un servidor de tickets.

d) -

37. En relación con el Single Sign On:

a) Los sistemas Web Single Sign On utilizan cookies para reconocer a los usuarios y su estado de autenticación

b) Los usuarios de los sistemas SSO mediante Kerberos reciben un ticket al registrarse que luego se presenta en las aplicaciones cliente

c) Las dos respuestas anteriores son correctas

d) Todas las respuestas anteriores son incorrectas

38. ¿Qué es SAML?

a) Un estándar abierto que define un esquema XML para el intercambio de datos de autenticación y autorización

b) Variante de UML especializada en el modelado de máquinas de estado

c) Lenguaje para la especificación de conjuntos de pruebas de software

d) Motor de enrutamiento y mediación basado en reglas que provee una implementación basada en objetos Java

39. A qué se denomina Single sign-on (SSO):

a) Procedimiento de cifrado para autenticar a un usuario

b) Procedimiento asociado al cifrado en Secure Sockets Layers (SSL)

c) Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación

d) Permite el acceso de los usuarios a servicios web a través del protocolo HTTPS

40. Kerberos es un protocolo de autenticación de redes de ordenador que:

a) Se basa en criptografía de clave simétrica y requiere un tercero de confianza.

b) Se basa en criptografía de clave asimétrica y requiere un tercero de confianza.

c) Se basa en criptografía de clave asimétrica y no requiere un tercero de confianza.

d) Se basa en criptografía de clave simétrica y no requiere un tercero de confianza.

41. La federación de identidades es:

a) la extensión de la gestión de la identidad a múltiples dominios de usuarios.

b) la extensión de la gestión de la identidad a múltiples dominios de seguridad.

c) la extensión de la gestión de la identidad a múltiples dominios de equipos.

d) la gestión integrada de la identidad para usuarios que pertenecen a la misma Unidad Organizativa.

42. SAML (Security Assertion Markup Language) es un estándar abierto basado en:

a) JavaScript.

b) Java.

c) XML.

d) C.

43. El protocolo Oauth:

a) Es propietario de Twitter, y permite gestionar el acceso a su API por parte de otras aplicaciones

b) Permite su uso en aplicaciones web y móviles, pero no en aplicaciones de escritorio

c) Permite el acceso a la identidad completa del usuario por parte del servidor de aplicaciones

d) Permite utilizar la cuenta de Facebook para acceder a otras aplicaciones

44. Es un software de metadirectorio:

a) Novell Directory Services

b) Open DS

c) Ganymede

d) Ninguno de los anteriores

45. Ventajas del teletrabajo:

a) Reducción de costes

b) Flexibilidad

c) Mejor planificación

d) Todas las respuestas anteriores son correctas

46. Indique cuál de las siguientes afirmaciones es correcta:

a) El sistema de autenticación "Kerberos", utiliza exclusivamente mecanismos de criptografía asimétrica

b) Para la autenticación "Kerberos" utiliza mecanismos basados en criptografía simétrica y en criptografía asimétrica

c) Para la autenticación "Kerberos" utiliza exclusivamente mecanismos basados en criptografía simétrica

d) Para la autenticación "Kerberos" utiliza mecanismos de identificación/password y de criptografía simétrica

47. ¿En qué RFC se define LDAPv3?

a) RFC 4511

b) RFC 5321

c) RFC 822

d) Aún continúa su implementación

48. ¿Qué es un sistema IDM (Identity Manager)?

a) Es una plataforma que permite gestionar desde un sólo punto el ciclo de vida de una identidad.

b) Es cualquier sistema de gestión de usuarios.

c) Es una plataforma de gestión de PKI para proporcionar tarjetas de identificación a los empleados de la organización.

d) Es una plataforma que impide la descentralización de la administración de los sistemas de control de acceso basados en roles.

49. En relación a SAML (Security Assertion Markup Language), señale la respuesta INCORRECTA:

a) Para la identificación del ciudadano, el modelo de federación de identidades de Cl@ve se basa en el estándar SAML 2.0.

b) Para facilitar la integración de aplicaciones y herramientas, el servicio común AutenticA incorpora SAML 2.0 a sus opciones de integración.

c) La especificación SAML define la estructura y el contenido de elementos como las aserciones, protocolos y perfiles.

d) Para proveer autenticación y confidencialidad, SAML no está diseñado para integrarse con XML Signature ni XML Encryption.

50. SAML (Security Assertion Markup Language):

a) Establece protocolos de seguridad para el intercambio de identidades.

b) Establece protocolos de seguridad para el firmado de estructuras XML.

c) Es un estándar establecido por IEEE como alternativa a WS-Security en sistemas de autenticación Single Sign-On.

d) Es un estándar establecido por OASIS como alternativa a WS-Security en sistemas de autenticación Single Sign-On.

51. En el ámbito del Single Sign-On, ¿cómo se denomina a la información confidencial agrupada (nombre de usuario, contraseña, etc) que se precisa para acceder a las aplicaciones?

a) Credenciales

b) Federación

c) Cookies

d) Login

52. Respecto al protocolo Oauth, señale la respuesta correcta:

a) Es propietario de Twitter, y permite gestionar el acceso a su API por parte de otras aplicaciones.

b) Permite su uso en aplicaciones web y móviles, pero no de escritorio.

c) Permite el acceso a la identidad completa del usuario por parte del servidor de aplicaciones.

d) Permite utilizar la cuenta de Facebook para acceder a otras aplicaciones.

53. ¿Qué es Single sign-on (SSO)?

a) Es un Sistema Operativo para proporcionar la autorización de utilización de recursos basado en certificados de usuario.

b) Es un método de control de acceso que permite a un usuario validarse una única vez y tener acceso a diferentes recursos sin tener que volver a introducir sus credenciales.

c) Es una plataforma que almacena todas las contraseñas del usuario para que éste no tenga que teclearlas cada vez que accede a las distintas aplicaciones.

d) Es la plataforma PM que emite certificados de empleado público para la Administraciones Locales y del Estado.

54. Acerca del protocolo Kerberos v5 (IETF RFC 4120):

a) Tiene extensiones que permiten el empleo de criptografía asimétrica.

b) Los tickets expiran tras un tiempo predeterminado en el protocolo.

c) El servidor de autenticación cifra el ticket que remite al cliente con una clave que obtiene a partir del nombre y la contraseña del usuario.

d) Utiliza los algoritmos de cifrado bajo el modo de operación denominado CBC (Cipher block chaining).

55. ¿Qué es SAML?

a) Un estándar abierto que define un esquema para el intercambio de datos de autenticación y autorización.

b) Un servicio proveedor de identidades.

c) Un protocolo para la verificación de identidades.

d) Un software de definición de autoridades.

56. La gestión de la identidad y de acceso en las organizaciones no se centra normalmente en una de las siguientes funciones:

a) Gestión de cuentas de usuario y contraseñas, siguiendo las directrices de las políticas de la empresa.

b) Gestión centralizada de los permisos de los usuarios, basada en directorios de usuarios (habitualmente basados en LDAP).

c) Para unir de forma segura dos redes locales separadas geográficamente o para unir un único equipo cliente a la red local remota de la organización.

d) Esquema de autorizaciones, que concentra en un solo punto las autorizaciones de acceso.

57. En Windows Server 2019, cuando se tienen grandes entornos, que tienen más de un dominio dentro de la misma red, ¿qué herramienta de gestión se utiliza para configurar el directorio activo?

a) Domains, Trees and Trusts

b) Active Directory Scope Expand

c) Active Directory Domains and Trusts

d) Active Directory Domains and Trees

58. ¿Qué es un metadirectorio?

a) Un directorio que genera directorios

b) Una implementación de LDAP

c) Un servicio de directorio puede, además, capturar los eventos que cada usuario realiza,

d) Es un software utilizado para replicar datos entre diferentes fuentes

59. En relación con las soluciones MDM (Mobile Device Management), señale la respuesta correcta:

a) En ningún caso contemplan la tendencia BYOD (Bring Your Own Device) que permite a los usuarios de una organización hacer uso de sus dispositivos móviles personales para el acceso al entorno, servicios y datos corporativos.

b) Sirven para gestionar la política de seguridad establecida en la organización no siendo adecuados para el inventario de dispositivos móviles.

c) Los fabricantes de las principales plataformas móviles no proporcionan soluciones MDM por lo que hay que recurrir siempre a soluciones de terceros.

d) Permiten la monitorización automática de los dispositivos móviles y la generación de alertas al incumplirse la política de seguridad establecida en la organización.

60. Cuando se utilizan soluciones de seguridad, Single Sign-On, los posibles atacantes de los servidores de una organización requerirían de (señale la respuesta INCORRECTA):

a) Conocimientos sobre técnicas criptográficas y de criptoanálisis.

b) Acceso a sistemas iguales para poder realizar pruebas/intentos de ataque.

c) Herramientas de análisis de redes y de explotación de vulnerabilidades.

d) Una mínima cantidad de tiempo para analizar los flujos de información intercambiados.

61. En el ámbito de la Gestión de Identidades, ¿cómo se denomina al conjunto de proveedores de servicios, identidades y atributos que disponen de acuerdos de servicio, comerciales y de negocio para que el usuario pueda realizar transacciones de forma transparente y sencilla entre todos ellos?

a) Web Access Management

b) WS - Security

c) Círculo de Confianza (CoT)

d) SAML

62. Su organización dispone de una aplicación que debe ser ofrecida a través de Internet, cuya estructura está separada en 4 capas: cliente pesado, capa web, capa de aplicación y capa de datos, ¿cómo publicaría dicha aplicación sin desplegar el cliente pesado en los puestos de usuario?

a) Virtualización de aplicaciones y escritorios.

b) VPN - Virtual Private Network.

c) Proxy inverso.

d) Ninguno de los anteriores.

63. Entre los requisitos de QoS en un sistema de videoconferencia, se encuentran…

a) Latencia, Resolución y Sonido envolvente

b) Latencia, Sonido envolvente y Tasa de pérdida de paquetes.

c) Resolución, Jitter y Tasa de pérdida de paquetes.

d) Latencia, Tasa de pérdida de paquetes y Jitter.

64. Uno de los grandes tipos en los que se puede clasificar la arquitectura de un SSO es la Arquitectura compuesta o federación, en la que se pueden utilizar distintos tipos de autenticación. Señale la respuesta INCORRECTA:

a) Autenticación basada en vales (tokens), con criptografía simétrica

b) Autenticación basada en PKI´s, con criptografía asimétrica

c) Autenticación múltiple mediante cacheo en cliente

d) Autenticación múltiple mediante cacheo en servidor utilizada, por ejemplo, en Kerberos

65. Son plataformas para el teletrabajo:

a) Freelancer.com

b) Nubelo

c) Workana.com

d) Todas las respuestas anteriores son correctas

66. Uno de los grandes tipos en los que se puede clasificar la arquitectura de un SSO es la Arquitectura compuesta o federación, en la que se pueden utilizar distintos tipos de autenticación. Señale la respuesta incorrecta:

a) Autenticación basada en vales (tokens), con criptografía simétrica.

b) Autenticación basada en PKI's, con criptografía asimétrica.

c) Autenticación múltiple mediante cacheo en cliente.

d) Autenticación múltiple mediante cacheo en servidor, utilizada por ejemplo en Kerberos.

67. Entre las funciones de un Application Delivery Controller (ADC) NO está:

a) Equilibrio de carga (Load balancing).

b) Protección de derechos de contenidos (Information Rights Management).

c) Cacheo de contenidos (Content caching).

d) Perfilado de tráfico (Traffic shaping).

68. Cuál de las siguientes tecnologías no está relacionada con la identificación y autentificación:

a) Certificados

b) Single Sign On

c) Kerberos

d) NetBios

69. En la gestión unificada de usuarios, ¿a qué se denomina Single Sign-On (SSO)?

a) Procedimiento de cifrado para autenticar a un usuario.

b) Procedimiento asociado al cifrado en Secure Socket Layer (SSL).

c) Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de autenticación.

d) Permite el acceso de los usuarios a servicios web a través del protocolo HTTPS.

70. Señale cuál de estas entidades no pertenece a una arquitectura SAML:

a) AP (Authentication Provider)

b) SP (Service Provider)

c) IdP (Identity Provider)

d) Todos los anteriores son componentes de la arquitectura SAML