Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PROCESO DE SELECCIÓN LIBRE PARA CUBRIR PLAZAS EN RÉGIMEN DE CONTRATO LABORAL EN MODALIDAD DE FIJO.

DOS plazas de INGENIERO AUXILIAR DE PROYECTOS (Nivel 12) en el DEPARTAMENTO DE CERES (1 plaza) y en la DIRECCIÓN DE SISTEMAS DE INFORMACIÓN (Área Digitalización-1 plaza)

OE: 06/22

AVISO

Una vez realizada y corregida la prueba teórica eliminatoria del presente proceso de selección, se han obtenido los resultados que se adjuntan al presente aviso.

Se establece plazo de solicitud de revisión de examen para los días 20, 21, 24, 25 y 26 de octubre de 2022, y el plazo de presentación de impugnaciones del 20 de octubre al 4 de noviembre de 2022. Los escritos deberán presentarse a través del Registro electrónico común de la Administración General del Estado con DNI electrónico o Certificado Digital: https://rec.redsara.es/registro/action/are/acceso.do

Asimismo, se convoca a las personas que han aprobado la prueba teórica eliminatoria, a la prueba de inglés no eliminatoria a las 9:00 horas del día 10 noviembre de 2022, y a la prueba práctica eliminatoria a las 12:30 horas del mismo día. Ambas pruebas se realizarán en el Centro de Formación de la FNMT-RCM.

Madrid, 19 de octubre de 2022
LA SECRETARIA DEL TRIBUNAL

OE 06/22 INGENIERO AUXILIAR DE PROYECTOS

Prueba teórica eliminatoria

REGISTRO	APELLIDOS, NOMBRE	NOTA
7900012262606	BAILAN ZAMORA, LIA	5,426
7900012373495	CARMONA TIRADO, AITOR	3,333
7900011833052	FRAILE LOPEZ, MIGUEL	1,938
7900011900155	GARCIA ESCARTIN, DAVID	6,279
7900012477996	GARCIA ESTEBAN, ANTONIO	6,008
7900011654026	GONZALEZ MARTIN, JAVIER	4,845
7900011565740	HERRANZ SANZ, MARIA	5,194
7900011870782	LAJUSTICIA AISA, ANGEL	4,380
7900011714436	LOPEZ PRIETO, SAMUEL	3,798
7900011528491	MARTIN GRANADOS, MARIA ANGELES	2,636
7900012254434	MARTINEZ GOMEZ, RUT	2,713
7900012169515	MOJONERO JIMENEZ, MIGUEL	4,186
7900012457881	NAVARRO BARRERO, LUCIA	3,527
7900012048616	PERDICES GUERRA, ALICIA	2,558
7900012395676	PEREZ DE LA FUENTE, MARIA ELENA	3,295
7900011496282	PINTO RODRÍGUEZ, ALBERTO	3,876
7900012327620	RINCON BONILLA, JUAN MANUEL	4,341
7900012428646	SACRISTAN ROMERO, FRANCISCO	3,178
7900012425103	SANTAMARIA VALLEJO, GUILLERMO	3,178
7900012026785	SANZ GARCIA, SERGIO	3,488
7900012357851	SEBASTIAN SEVILLA, SALVADOR	5,116
7900012394601	SEGURA BRAVO, RUTH	3,992
7900011656722	TOLBAÑOS GRANJO, LAURA	4,690

HOJA DE RESPUESTAS CORRECTAS

Código Exámen: 0 6 1 2 2

Número de preguntas: 0 8 6

Número de Respuestas: 3

Instrucciones:
1-. Asígnele un código de 5 cifras al exámen.
2-. Indique el número de preguntas del exámen.
3-. En el caso de que todas las preguntas tengan el mismo número de respuestas indique este número en la cabecera. En el caso que alguna pregunta contenga un número de respuestas diferente indíquelo en la opción contigua a la respuesta.
4-. Si desea que los fallos resten puntos seleccione la opción más apropiada.

Opciones: Si hay n respuestas posibles los fallos restan

○ 1/(n-1) Puntos ● 1/3 Punto ○ 1/5 Punto
○ 1/2 Punto ○ 1/4 Punto

	Respuesta Correcta	Número de Respuestas
	A B C D E F	2 3 4 5 6
1	○○●○○○	○○○○○
2	○○●○○○	○○○○○
3	○○●○○○	○○○○○
4	●○○○○○	○○○○○
5	●○○○○○	○○○○○
6	○●○○○○	○○○○○
7	●○○○○○	○○○○○
8	○○●○○○	○○○○○
9	●○○○○○	○○○○○
10	○●○○○○	○○○○○
11	○○●○○○	○○○○○
12	○●○○○○	○○○○○
13	●○○○○○	○○○○○
14	○○●○○○	○○○○○
15	●○○○○○	○○○○○
16	●○○○○○	○○○○○
17	○○●○○○	○○○○○
18	○○●○○○	○○○○○
19	●○○○○○	○○○○○
20	○○●○○○	○○○○○
21	●○○○○○	○○○○○
22	○○●○○○	○○○○○
23	○●○○○○	○○○○○
24	●○○○○○	○○○○○
25	●○○○○○	○○○○○
26	○○●○○○	○○○○○
27	○●○○○○	○○○○○
28	○●○○○○	○○○○○
29	●○○○○○	○○○○○
30	○●○○○○	○○○○○
31	○○●○○○	○○○○○
32	○●○○○○	○○○○○
33	○○●○○○	○○○○○
34	●○○○○○	○○○○○
35	○●○○○○	○○○○○
36	○○●○○○	○○○○○
37	●○○○○○	○○○○○
38	○●○○○○	○○○○○
39	●○○○○○	○○○○○
40	●○○○○○	○○○○○
41	○●○○○○	○○○○○
42	○○●○○○	○○○○○
43	○○●○○○	○○○○○
44	○●○○○○	○○○○○
45	○●○○○○	○○○○○
46	●○○○○○	○○○○○
47	○○●○○○	○○○○○
48	○○●○○○	○○○○○
49	○○●○○○	○○○○○
50	●○○○○○	○○○○○

	Respuesta Correcta	Número de Respuestas
	A B C D E F	2 3 4 5 6
51	○●○○○○	○○○○○
52	○●○○○○	○○○○○
53	○●○○○○	○○○○○
54	●○○○○○	○○○○○
55	○○●○○○	○○○○○
56	○●○○○○	○○○○○
57	●○○○○○	○○○○○
58	○○●○○○	○○○○○
59	○○●○○○	○○○○○
60	●○○○○○	○○○○○
61	○●○○○○	○○○○○
62	○○●○○○	○○○○○
63	○○●○○○	○○○○○
64	●○○○○○	○○○○○
65	●○○○○○	○○○○○
66	○●○○○○	○○○○○
67	○○●○○○	○○○○○
68	○●○○○○	○○○○○
69	●○○○○○	○○○○○
70	○○●○○○	○○○○○
71	○●○○○○	○○○○○
72	○○●○○○	○○○○○
73	●○○○○○	○○○○○
74	○●○○○○	○○○○○
75	○●○○○○	○○○○○
76	○●○○○○	○○○○○
77	○○●○○○	○○○○○
78	●○○○○○	○○○○○
79	○●○○○○	○○○○○
80	○○●○○○	○○○○○
81	○●○○○○	○○○○○
82	●○○○○○	○○○○○
83	○○●○○○	○○○○○
84	○○●○○○	○○○○○
85	●○○○○○	○○○○○
86	○○●○○○	○○○○○
87	○○○○○○	○○○○○
88	○○○○○○	○○○○○
89	○○○○○○	○○○○○
90	○○○○○○	○○○○○
91	○○○○○○	○○○○○
92	○○○○○○	○○○○○
93	○○○○○○	○○○○○
94	○○○○○○	○○○○○
95	○○○○○○	○○○○○
96	○○○○○○	○○○○○
97	○○○○○○	○○○○○
98	○○○○○○	○○○○○
99	○○○○○○	○○○○○
100	○○○○○○	○○○○○

	Respuesta Correcta	Número de Respuestas
	A B C D E F	2 3 4 5 6
101	○○○○○○	○○○○○
102	○○○○○○	○○○○○
103	○○○○○○	○○○○○
104	○○○○○○	○○○○○
105	○○○○○○	○○○○○
106	○○○○○○	○○○○○
107	○○○○○○	○○○○○
108	○○○○○○	○○○○○
109	○○○○○○	○○○○○
110	○○○○○○	○○○○○
111	○○○○○○	○○○○○
112	○○○○○○	○○○○○
113	○○○○○○	○○○○○
114	○○○○○○	○○○○○
115	○○○○○○	○○○○○
116	○○○○○○	○○○○○
117	○○○○○○	○○○○○
118	○○○○○○	○○○○○
119	○○○○○○	○○○○○
120	○○○○○○	○○○○○
121	○○○○○○	○○○○○
122	○○○○○○	○○○○○
123	○○○○○○	○○○○○
124	○○○○○○	○○○○○
125	○○○○○○	○○○○○
126	○○○○○○	○○○○○
127	○○○○○○	○○○○○
128	○○○○○○	○○○○○
129	○○○○○○	○○○○○
130	○○○○○○	○○○○○
131	○○○○○○	○○○○○
132	○○○○○○	○○○○○
133	○○○○○○	○○○○○
134	○○○○○○	○○○○○
135	○○○○○○	○○○○○
136	○○○○○○	○○○○○
137	○○○○○○	○○○○○
138	○○○○○○	○○○○○
139	○○○○○○	○○○○○
140	○○○○○○	○○○○○
141	○○○○○○	○○○○○
142	○○○○○○	○○○○○
143	○○○○○○	○○○○○
144	○○○○○○	○○○○○
145	○○○○○○	○○○○○
146	○○○○○○	○○○○○
147	○○○○○○	○○○○○
148	○○○○○○	○○○○○
149	○○○○○○	○○○○○
150	○○○○○○	○○○○○

64374

OE 06/22 INGENIERO AUXILIAR DE PROYECTOS

PRUEBA TEÓRICA ELIMINATORIA (TIPO TEST)

---

1. **Cuando hablamos de un incidente de seguridad, ¿Cuál de las siguientes afirmaciones NO se consideran ciertas?**
   a) Es imposible predecir un incidente.
   b) Es muy posible que el impacto asociado a un incidente sea alto.
   c) Es muy posible predecir un incidente.
2. **Ante un incidente de seguridad, ¿Cuál de los siguientes criterios de determinación NO se considera como un nivel de Impacto Potencial CRITICO?**
   a) Afecta a una Infraestructura Crítica
   b) Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios
   c) Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
3. **¿Qué objetivo NO persigue la plataforma LUCIA?**
   a) Ser conforme con los requisitos del Esquema Nacional de Seguridad (ENS).
   b) Reportar al CCN-CERT la información de contexto (metadatos) de los ciberincidentes identificados en los organismos.
   c) Detección de malware complejo y movimiento lateral relacionado con APT.
4. **¿Qué se entiende por DDoS?**
   a) Se entiende como un ataque de denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo.
   b) Se entiende como un ataque sobre un servidor web como consecuencia del cual se cambia su apariencia.
   c) Se entiende por un ataque con un programa que está diseñado para copiarse y propagarse por sí mismo mediante mecanismos de red.
5. **¿Qué tipo de incidente se puede clasificar como de "Obtención de Información"?**
   a) Sniffing
   b) Servidor C&C
   c) Phising
6. **Según la guía CCN-STIC-817, ¿Cuál sería el "nivel de impacto potencial" determinado de un ciberincidente sufrido en una organización que ha interrumpido la presentación servicio durante más de 1 hora y afectando a más del 10% de usuarios?**
   a) Critico
   b) Alto
   c) Muy Alto
7. **¿Cómo se denomina el uso fraudulento de sitios web o correos electrónicos, que simulan ser una entidad bancaria o empresa de confianza, con el fin de obtener el nombre del usuario y contraseña de acceso?**
   a) Phishing
   b) Roaming
   c) Pharming
8. **¿Qué problema resuelve el WEP dinámico?**
   a) Reutilización de vectores de inicialización
   b) Posibilidad de inyectar tráfico
   c) Autenticación en la red

9. ¿El protocolo HTTPS..?

a) Crea un canal cifrado entre el cliente y servidor, mediante el uso de SSL/TLS y el puerto TCP/443
b) Crea un canal cifrado entre el cliente y servidor, mediante el uso de SSL/TLS y el puerto TCP/80
c) Crea un canal cifrado entre el cliente y servidor, mediante el uso de SSL/TLS y el puerto TCP/110

10. ¿Cuáles son las diferencias entre el protocolo TCP y UDP?

a) UDP es un protocolo orientado a conexión, a diferencia de TCP, que es sin conexión. Solo el protocolo UDP añade fiabilidad, recuperación de errores y el control de flujo.
b) TCP es un protocolo orientado a conexión, a diferencia de UDP, que es sin conexión. Solo, el protocolo TCP añade fiabilidad, recuperación de errores y el control de flujo.
c) TCP es un protocolo orientado a conexión, a diferencia de UDP, que es sin conexión. Ambos protocolos añaden fiabilidad, recuperación de errores y el control de flujo.

11. Indica cuál de las siguientes afirmaciones es FALSA:

a) S-MIME es un protocolo de seguridad a nivel de aplicación, pero su uso se limita a la protección del correo electrónico mediante el cifrado y las firmas digitales. Se basa en tecnología de clave pública y utiliza certificados X.509 para establecer la identidad de las partes que se comunican.
b) El Framework IPSec es un conjunto de protocolos cuyo objetivo es asegurar las comunicaciones, autenticando y cifrando cada paquete IP. IPSec dispone de dos modos de funcionamiento, túnel y transporte. El protocolo AH proporciona autenticidad de origen, integridad y protección de confidencialidad.
c) El protocolo SMTP es un protocolo basado en texto de transferencia de archivos entre sistemas basado en una arquitectura cliente-servidor. Toda la comunicación entre ambos extremos, incluida la autenticación, se realiza en texto claro.

12. ¿Cuál de las siguientes afirmaciones se consideraría una desventaja del uso de la planificación de un proyecto?

a) Requiere actividades con orden y propósito.
b) La planificación está limitada por la exactitud de la información y de los hechos futuros.
c) Obliga a la visualización del conjunto

13. ¿Qué es el CISO?

a) Persona responsable de la seguridad de la información de una organización.
b) Pieza de software que permite a un "operador" controlar a distancia un sistema como si se tuviera acceso físico al mismo.
c) Un tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.

14. ¿Cuál de las siguientes actividades NO determinan el tipo de inspección de seguridad?

a) Análisis
b) Verificación
c) Validación

15. ¿Qué información mínima debe contener el informe técnico de una inspección de seguridad para cada vulnerabilidad relevante detectada?

a) Identificación, acciones ejecutadas, evidencia, impacto, solución y gravedad.
b) Identificación, líneas de trabajo recomendadas, fechas y personal de contacto.
c) Identificación, nivel de riesgo, acciones ejecutadas, fechas y personal de contacto.

16. ¿Dónde se establecen las reglas generales que se deben seguir o a las que se deben de ajustar las conductas, tareas o actividades de las personas y Organizaciones en relación con la protección de la información cuando es manejada por un sistema?

a) Normas STIC
b) Instrucciones Técnicas STIC
c) Procedimientos STIC

17. Indique la respuesta CORRECTA que resume el funcionamiento de la firma digital con criptografía de clave pública, garantizando autenticidad del origen, el no repudio en origen y la integridad

a) El emisor calcula un hash del mensaje, cifra el resultado de la función hash con su clave pública y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza la clave privada del emisor para descifrar el criptograma.
b) El emisor calcula un hash del mensaje, cifra el resultado de la función hash con su clave privada y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza su clave privada para descifrar el criptograma.
c) El emisor calcula un hash del mensaje, cifra el resultado de la función hash con su clave privada y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza la clave pública del emisor para descifrar el criptograma.

18. Según el manual CCN-STIC-400, ¿Cuál de las siguientes funciones NO es responsabilidad de los operadores?

a) Recibir en primera instancia las incidencias que se produzcan, notificadas por usuarios.
b) Se encargan de la operación continua de los servicios TIC.
c) Se encargan de la instalación y configuración de aplicaciones, equipos y comunicaciones.

19. Según el manual CCN-STIC-400, el comité de seguridad corporativa

a) Centraliza toda la gestión de la seguridad de la Organización en sus diferentes ámbitos con objeto de proteger el servicio de forma correcta, completa y eficiente.
b) Aprueba la Política de Seguridad de la Organización.
c) Es el responsable de coordinar la respuesta ante incidentes que desborden los casos previstos y procedimentados. Es el responsable de coordinar la investigación forense relacionada con incidentes que se consideren relevantes.

20. En caso de desastre, ¿Quién se incorpora al Comité de Crisis y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la Organización?

a) Alta Dirección
b) Responsable de Seguridad Corporativa
c) Administrador STIC

21. Si Carmen quiere transmitir un documento cifrado (sin autenticación) hacia Luis utilizando un algoritmo de clave asimétrica:

a) Debe cifrarlo con la clave pública de Luis.
b) Debe cifrarlo con la clave privada de Luis.
c) Debe cifrarlo con la clave privada de Carmen.

22. ¿Quién es el responsable de indicar el estado de revocación de los certificados que emite una Autoridad de Certificación?

a) La Autoridad de Registro o RA
b) La Autoridad de Sellado de Tiempo o TSA
c) La Autoridad de Certificación o CA

23. Seleccione la afirmación ERRÓNEA según la RFC 5280:

a) La indicación de un certificado revocado se publica en la siguiente CRL que se emita y en las posteriores hasta que finalice el período de validez inicial del certificado revocado.
b) La indicación de que un certificado ha sido revocado se publica en la primera CRL que se emita, pero no es necesario publicarla en las posteriores. Por lo que es necesario para verificar la validez de un certificado que se compruebe que no se indique su revocación en ninguna CRL emitida tras la emisión del certificado hasta la fecha.
c) Un certificado electrónico puede no ser válido en el momento de emisión.

24. ¿Cuál de las siguientes afirmaciones es FALSA?

a) El campo signatureValue de un certificado contiene la firma digital de los campos "tbsCertificate" y "signatureAlgorithm"
b) Para poder verificar un certificado electrónico y su camino de certificación (certification path) según el algoritmo básico para validar caminos de certificación descrito en la RFC 5280, es necesario que el sistema que realiza la validación (navegador web, sistema operativo, etc) cuente con un anclaje de confianza (trust anchor) para dicho camino de certificación. Éste puede ser el certificado raíz de una jerarquía de CAs
c) Un certificado electrónico, según la RFC 5280, contiene una firma electrónica mediante criptografía de clave pública de los datos a ser firmados (los nombres del sujeto y del emisor, una clave pública asociada al sujeto, un período de validez y otra información asociada)

25. Seleccione la afirmación CORRECTA:

a) Una respuesta correcta según el protocolo OCSP debe ir firmada digitalmente, en todos los casos.
b) Una respuesta correcta según el protocolo OCSP no necesita ir firmada digitalmente si se transmite mediante https, ya que de esta forma se puede verificar la identidad del servidor y se garantiza confidencialidad e integridad.
c) Una respuesta correcta según el protocolo OCSP puede incluir referencias a una CRL que contenga información del estado de un certificado concreto.

26. Seleccione la afirmación ERRÓNEA:

a) Si un servicio OCSP sabe que la clave privada de una CA en particular ha sido comprometida, puede devolver el estado "revocado" para todos certificados emitidos por esa CA, aunque los certificados no hubieran sido revocados explícitamente.
b) Antes de aceptar como válida una respuesta de un servicio OCSP para un certificado en particular, los clientes OCSP deberán confirmar que el certificado identificado en una respuesta recibida corresponde a el certificado que se identificó en la solicitud correspondiente y que la firma en la respuesta es válida.
c) Una petición a un servicio OCSP debe ir firmada digitalmente, en todos los casos.

27. Si se realiza una firma básica (CAdES - BES) de un documento con un certificado cualificado que caduca en un año… (seleccione la afirmación CORRECTA)

a) la firma seguirá siendo válida transcurrido un año gracias a que el formato tenía formato CAdES – BES.
b) para que se pueda verificar la validez de la firma transcurrido un año con plenas garantías jurídicas puede ser convertida a formato CAdES – A antes de que deje de ser válido el certificado.
c) para que se pueda verificar la validez de la firma transcurrido un año con plenas garantías jurídicas puede ser convertida a formato PAdES – BES antes de que deje de ser válido el certificado.

28. ¿Cuál de los siguientes formatos de firma no incluye sellado de tiempo?

a) AdES A
b) AdES – BES
c) AdES C

29. Señale la afirmación ERRÓNEA de acuerdo a la Declaración General de Prácticas de Certificación de la FNMT-RCM

a) El Suscriptor de un Certificado se corresponde siempre con la figura de Firmante. Los Firmantes son las personas físicas que mantienen bajo su uso exclusivo los Datos de creación de firma asociados a los Certificados.
b) Las partes que confían son aquellas personas físicas o jurídicas, diferentes del Firmante / Suscriptor, que reciben y / o usan Certificados expedidos por la FNMT-RCM y, como tales, les es de aplicación lo establecido por la correspondiente DPC cuando deciden confiar efectivamente en tales Certificados.
c) No se podrán emplear los Certificados de entidad final expedidos por la FNMT-RCM para usos particulares o privados, salvo para relacionarse con las Administraciones cuando éstas lo admitan.

30. La FNMT – RCM, a través de su Comité de Gestión del Prestador de Servicios de Confianza, vela por el cumplimiento de las Declaraciones de Políticas y Prácticas de Certificación, las aprueba y realiza el pertinente proceso de revisión de las mismas, con una periodicidad...

a) semestral
b) anual
c) bianual

31. Seleccione la afirmación ERRÓNEA según la Declaración General de Prácticas de Certificación de la FNMT-RCM

a) Para identificar cada una de las Políticas de Certificación se disponen de OIDs específicos.
b) Los miembros de la Comunidad Electrónica y los Usuarios de los servicios tienen la obligación comprobar regularmente los documentos declarativos correspondientes (Políticas y/o Prácticas de Certificación de aplicación), solicitando cuanta información consideren oportuna a la FNMT-RCM.
c) El término Certificado de firma electrónica se define como una declaración electrónica que vincula los Datos de Creación de una firma, o clave privada, con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.

32. Un Certificado cualificado de firma electrónica se define en la Declaración General de Prácticas de Certificación de la FNMT-RCM como un Certificado electrónico emitido por un Prestador de Servicios de Confianza cumpliendo los requisitos establecidos en…

a) La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
b) El Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
c) El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su Capítulo III. Política de seguridad y requisitos mínimos de seguridad.

33. Seleccione la afirmación correcta en relación con la Validación inicial de la identidad que se realiza de acuerdo a la Declaración General de Prácticas de Certificación de la FNMT-RCM

a) Todos los nombres distintivos (DN) del campo Subject Name son significativos. La descripción de los atributos asociados al Suscriptor del Certificado no es legible por humanos. Su codificación permite la validación del certificado a los sistemas automatizados.
b) La autenticación de la identidad de la persona física solicitante se realizará, en todos los casos, mediante la personación física en la Oficina de Registro con el documento oficial correspondiente acreditativo de la identidad de la persona y según la legislación vigente.
c) En los casos en los que en el Certificado se incluyan datos como nombres de dominio o direcciones IP, la FNMT – RCM comprobará, a través de los sistemas de información que los registradores autorizados para cada caso pongan a disposición del público, que la documentación exigida y validada por la Oficina de Registro es la correcta.

34. Según la Declaración General de Prácticas de Certificación de la FNMT-RCM, ¿Cuándo se hace efectiva la solicitud de revocación de un certificado electrónico?

a) En el momento de verificar la identidad del Titular o, en su caso, de la veracidad de la solicitud realizada mediante resolución judicial o administrativa.
b) El siguiente día natural tras verificar la identidad del Titular o, en su caso, de la veracidad de la solicitud realizada mediante resolución judicial o administrativa.
c) Con la publicación cada 24h de la consiguiente CRL que contiene la referencia al certificado objeto de revocación tras verificar la identidad del Titular o, en su caso, de la veracidad de la solicitud realizada mediante resolución judicial o administrativa.

35. Según la Declaración General de Prácticas de Certificación de la FNMT-RCM, ¿cuál es la frecuencia de generación de CRLs de los Certificados de entidad final?

a) Sólo cuando se produce una nueva revocación
b) Al menos cada 12 horas
c) Al menos cada 24 horas

36. La FNMT-RCM, en su actividad de Prestador de Servicios de Confianza…(seleccione la afirmación ERRÓNEA)

a) Registrará todos aquellos eventos significativos con el fin de verificar que todos los procedimientos internos necesarios para el desarrollo de la actividad se ejecutan de acuerdo a la Declaración General de Prácticas de Certificación de la FNMT-RCM, a la normativa legal aplicable, y a lo establecido en el Plan de Seguridad Interna de FNMT-RCM y en los Procedimientos de Calidad y Seguridad, y permitir detectar las causas de posibles anomalías.
b) Pondrá a disposición de las autoridades competentes las evidencias relativas a los eventos registrados que obren en su poder, mediante requerimiento judicial o el correspondiente procedimiento legal, previa solicitud por escrito.
c) Publicará en el repositorio LDAP de acceso público la citada base con las evidencias relativas a los eventos registrados que obren en su poder. En caso de ocurrir algún fallo en la secuencia descrita, se produce una alarma al objeto de subsanar el posible error.

37. Seleccione la afirmación falsa relativa a la Generación del par de Claves de la CA

a) Por motivos de seguridad y calidad, las Claves que la FNMT-RCM necesita para el desarrollo de su actividad como Prestador de Servicios de Confianza, serán generadas por el Ministerio de Industria, Comercio y Turismo dentro de su propia infraestructura en un entorno físico seguro y al menos por dos personas autorizadas para ello.
b) La generación de las Claves y la protección de la Clave Privada, se realizan garantizando las necesarias medidas de confidencialidad, usando sistemas de hardware y software seguros y de confianza conforme a las normas EESSI CWA14167-1 y CWA14167-2.
c) Se elabora un informe que demuestra que la ceremonia correspondiente se ha llevado a cabo de conformidad con el procedimiento establecido, y que se garantizan la integridad y la confidencialidad del par de claves. Dicho informe es firmado por las personas que ejercen los correspondientes roles de confianza en la generación de Claves de una AC subordinada, y en el caso de una AC raíz será firmado adicionalmente por auditor confiable e independiente del equipo de gestión del Prestador.

38. Selecciona la afirmación CORRECTA respecto a la criptografía simétrica

a) El algoritmo de cifrado triple DES utiliza una longitud de clave típica de 2048 bits
b) Los algoritmos de clave simétrica no utilizan una clave pública para descifrado de los mensajes
c) Se puede utilizar RSA como algoritmo de clave simétrica

39. Selecciona la afirmación incorrecta respecto a la criptografía asimétrica

a) La firma electrónica se realiza con los certificados electrónicos y la clave contenida en éstos.
b) Cuanto mayor sea la longitud de la clave, menor es el rendimiento de la operación.
c) El algoritmo RSA, aparte de operaciones de firma digital, también nos permite realizar operaciones de cifrado.

40. Selecciona la afirmación correcta respecto a la criptografía asimétrica

a) Para cifrar datos para un tercero utilizamos su clave pública
b) Para cifrar datos para un tercero utilizamos su clave privada
c) No se puede cifrar datos con criptografía asimétrica

41. La obligación de reconocer los medios de identificación electrónica en el acceso a servicios en línea habrá de aplicarse únicamente cuando el organismo del sector público en cuestión emplee un nivel de seguridad:

a) Bajo, sustancial o alto.
b) Sustancial o alto.
c) Alto.

42. En relación a los sistemas de identificación electrónica, los estados miembros de la UE:

a) Están obligados a notificar todos sus sistemas de identificación electrónica a la Comisión para el acceso a los servicios públicos en línea.
b) La Comisión determina qué sistemas de identificación deben ser notificados por cada estado miembro, ya sea para el acceso a servicios públicos o privados.
c) Corresponde a los estados miembros decidir si notifican todos, algunos o ninguno de los sistemas de identificación electrónica utilizados a nivel nacional para el acceso al menos a los servicios públicos en línea o a servicios específicos.

43. El reglamento (UE) 910/2014 establece un marco jurídico general para la utilización de los servicios de confianza y, a tal efecto, recomienda:

a) Que dicho reglamento debe crear la obligación general de utilizarlos y de instalar un punto de acceso para todos los servicios de confianza existentes.
b) Que dicho reglamento debe crear la obligación general de utilizarlos, si bien no se debe exigir la instalación de un punto de acceso para todos los servicios de confianza.
c) Que dicho reglamento no debe crear la obligación general de utilizarlos ni de instalar un punto de acceso para todos los servicios de confianza existentes.

44. Según establece el reglamento (UE) 910/2014 en lo relativo a la definición de los servicios de confianza cualificados:

a) Debe asegurarse que la lista cerrada de los servicios de confianza previstos en dicho reglamento son los únicos que pueden ser utilizados a efectos de su reconocimiento a nivel nacional como servicios de confianza cualificados.
b) Los estados miembro deben conservar la libertad para definir otros servicios de confianza, además de los que forman parte de la lista cerrada de los servicios de confianza prevista en el reglamento, a efectos de su reconocimiento a nivel nacional como servicios de confianza.
c) El reglamento no establece nada sobre la obligatoriedad o falta de ella en lo relativo al uso de los servicios de confianza cualificados previstos en dicho reglamento.

45. El reglamento (UE) 910/2014 establece la necesidad de crear una etiqueta de confianza <<UE>> que permita identificar los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza. El uso de la etiqueta de confianza por parte de los prestadores cualificados de servicios de confianza:

a) Es obligatorio.
b) Es voluntario y no debe implicar más requisitos que los establecidos en el citado reglamento.
c) Es voluntario, si bien aquellos prestadores que decidan utilizarla deben superar las exigencias sobre seguridad y calidad del servicio establecidos en la decisión 2009/767/CE.

46. La suspensión de certificados cualificados es una práctica operativa establecida de los prestadores de servicios de confianza, distinta de la revocación y que conlleva la pérdida temporal de la validez de un certificado. En relación a esta práctica, el reglamento (UE) 910/2014 establece:

a) Que no se debe imponer el uso de la suspensión, pero deben de establecerse normas de transparencia donde y cuando esta práctica sea posible.
b) Impone el servicio de suspensión, al considerar que la revocación de un certificado constituye una medida desproporcionada de cara a afrontar problemas leves de seguridad.
c) Permite el uso de la suspensión, pero sólo para el caso de los certificados de empleado público.

47. Una empresa desea utilizar un sello electrónico para autenticar un software de copias de seguridad diseñado e implementado por la propia empresa. Esa práctica:

a) No es correcta porque los sellos electrónicos sólo pueden ser utilizados para autenticar documentos expedidos por una persona jurídica y un software no entra dentro de esta categoría.
b) No es correcta porque resulta imposible generar una firma avanzada de un software.
c) Es correcta porque los sellos electrónicos pueden ser utilizados para autenticar documentos electrónicos o cualquier activo digital de la persona jurídica, tales como programas informáticos, servidores, etc.

48. Según el reglamento (UE) 910/2014, un prestador de servicios de confianza puede ser:

a) Sólo una persona física.
b) Sólo una persona jurídica.
c) Una persona física o jurídica.

49. Según el reglamento (UE) 910/2014 los prestadores de servicios de confianza serán auditados:

a) Por un organismo de evaluación de la conformidad y al menos cada 24 meses, con independencia de que sean prestadores cualificados o no cualificados.
b) Por un organismo de evaluación de la conformidad, cada 12 meses para el caso de prestadores cualificados y cada 24 meses para el caso de los prestadores no cualificados.
c) Por un organismo de evaluación de la conformidad y al menos cada 24 meses, pero sólo para el caso de los prestadores cualificados.

50. La NTI de Política de firma y sello electrónicos y de certificados de la administración establece que el creador de un sello es:

a) Una persona jurídica que crea un sello electrónico.
b) Una persona física o jurídica que crea un sello electrónico.
c) Un autómata que mediante procedimientos automatizados crea un sello electrónico.

51. En lo relativo a las firmas electrónicas de contenido, la NTI establece:

a) La utilización obligatoria de los formatos de firma XAdES, CAdES y PAdES.
b) Por compatibilidad, se permiten aunque no se recomiendan los formatos XAdES, CAdES y PAdES.
c) La NTI no hace mención a formatos específicos de firma electrónica.

52. Una firma XAdES-T Level es:

a) Una firma que permite la verificación de las firmas electrónicas en el largo plazo y sin límite de tiempo.
b) Una firma que permite la verificación de las firmas electrónicas, aunque se haya producido la revocación del certificado firmante, pero no permite realizar la validación de las mismas una vez se haya producido la caducidad del certificado firmante.
c) No existe el formato XAdES-T Level de firma electrónica.

53. La especificación del TSP (Time Stamp protocol) recogida en la RFC3161 especifica:

a) Los mensajes, codificados en ASN.1, que deben intercambiar las TSA y los solicitantes de tokens de time-stamp, sin entrar en detalles relativos a los mecanismos de transporte a emplear para realizar la transmisión de los mensajes.
b) Los mensajes codificados en ASN.1 que deben intercambiar las TSA y los solicitantes de tokens de time-stamp, así como una descripción de determinados mecanismos de transporte que pueden ser empleados a tal efecto, siempre de manera opcional y dejando claro que en el futuro podrán definirse mecanismos adicionales.
c) La RFC3161 es una especificación de alto nivel que no recoge detalle alguno del TSP que debe ser utilizado entre las TSA y los solicitantes de tokens de time-stamp.

54. De acuerdo con lo establecido en la RFC3161, los token de time-stamp generados por una TSA:

a) Deben estar firmados utilizando una clave generada específicamente para este fin, para lo cual deberá establecerse la correspondiente propiedad de la clave en el certificado electrónico correspondiente.
b) Deben estar firmados utilizando una clave vinculada a un certificado digital, no requiriéndose condiciones particulares para la expedición de este certificado salvo que la titularidad del mismo sea ostentada por la TSA generadora del token.
c) En forma alguna se exige la firma de los tokens de time-stamp generados por una TSA mediante un certificado digital, pudiéndose, en su lugar, incorporar al token un CSV (Código Seguro de Verificación).

55. Las consideraciones generales sobre las reglas de confianza de firmas longevas recogidas en la NTI (Norma Técnica de Interoperabilidad) establecen que, para la incorporación a la firma de información completa de validación, se usará validación:

a) Sólo mediante OCSP.
b) Sólo mediante CRLs.
c) Mediante CRLs u OCSP.

56. La NTI establece condiciones para políticas de firma y sello electrónico:

a) Basadas en el uso de certificados digitales, advirtiendo de la necesidad obligada de utilizar siempre certificados digitales.
b) Basadas en el uso de certificados digitales, si bien la NTI no incluye ninguna limitación que impida incluir en la política de firma y sello, además de lo establecido para firmas con certificados, otros sistemas de firmas recogidos en la legislación, tales como CSV, claves concertadas u otros sistemas no criptográficos.
c) La NTI no establece condición alguna para políticas de firma y sello electrónico.

57. Según la NTI de Documento Electrónico, ¿cuál de los siguientes componentes NO forma parte de un Documento Electrónico?

a) Índice electrónico.
b) Firma electrónica.
c) Metadatos.

58. ¿Cuáles son los sistemas que pueden ser utilizados para la firma electrónica por parte de las organizaciones según la ley 40/2015, de 1 de octubre?

a) Sistema de sello electrónico reconocido y Código Seguro de Verificación (CSV).
b) Firma electrónica basada en certificados y Sistema de sello electrónico reconocido.
c) Firma electrónica basada en certificados y Código Seguro de Verificación (CSV).

59. Según la NTI de Documento Electrónico, ¿qué afirmación es FALSA respecto a los metadatos mínimos obligatorios de un Documento Electrónico?

a) No serán modificados en ninguna fase posterior del procedimiento administrativo, a excepción de modificaciones necesarias para la corrección de errores u omisiones en el valor inicialmente asignado.
b) Estarán presentes en cualquier proceso de intercambio de documentos electrónicos entre órganos de la Administración y Entidades de Derecho Público vinculadas o dependientes de aquélla y con el ciudadano.
c) Serán implementados por cada órgano de la Administración en su propio ámbito de actuación.

60. Según la NTI de Documento Electrónico, ¿cuáles de los siguientes son metadatos mínimos obligatorios de un Documento Electrónico?

a) Órgano, Tipo documental y Tipo de firma.
b) Versión NTI, Idioma y Nombre de formato.
c) Origen, Identificador y Resolución.

61. Según la NTI de Documento Electrónico, ¿cuál es la estructura normalizada correcta del metadato "Identificador" del Documento Electrónico?

a) ES_<AAAA>_<Órgano>_<ID_específico>
b) ES_<Órgano>_<AAAA>_<ID_específico>
c) ES_<Órgano>_<ID_específico>_<AAAA>

62. Según la NTI de Documento Electrónico, ¿qué indica el metadato "Estado de elaboración" del Documento Electrónico?

a) Indica si el contenido del documento fue creado por el ciudadano o por una administración.
b) Indica si el documento ha sido consultado, modificado, revisado o aprobado.
c) Indica la naturaleza del documento. Si es original o copia, y el tipo de copia.

63. Según la NTI de Documento Electrónico, ¿qué indica el metadato mínimo obligatorio "Origen" de un Documento Electrónico?

a) Indica el organismo que crea o digitaliza el documento.
b) Indica el lugar de procedencia del documento.
c) Indica si el contenido del documento fue creado por un ciudadano o por una administración.

64. Según la NTI de Documento Electrónico, ¿cómo se define la Autenticidad?

a) Referido a un documento, propiedad que puede atribuírsele como consecuencia de que puede probarse que es lo que afirma ser, que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado, y que ha sido creado o enviado en el momento en que se afirma, sin que haya sufrido ningún tipo de modificación.
b) Referido a un documento, propiedad o característica que indica que su contenido puede ser considerado una representación completa y precisa de las actuaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores actuaciones o actividades.
c) Referido a un documento, propiedad o característica que indica su carácter de completo, sin alteración de ningún aspecto esencial.

65. De los siguientes componentes, ¿cuál se desarrolla en la NTI de Digitalización de Documentos?

a) Requisitos mínimos de conservación y disponibilidad de los documentos digitalizados.
b) Procedimiento formal de digitalización.
c) Proceso de generación de copias electrónicas auténticas de documentos en soporte papel.

66. ¿Cuál es el nivel de resolución mínimo que establece la NTI de Digitalización de Documentos para Imágenes Electrónicas?

a) 300 ppp tanto para imágenes obtenidas en blanco/negro, escala de grises o color.
b) 200 ppp tanto para imágenes obtenidas en blanco/negro, escala de grises o color.
c) 300 ppp para imágenes obtenidas en blanco/negro y escala de grises y 200 ppp para imágenes obtenidas en color.

67. Según la NTI de Expediente Electrónico, ¿cuáles son los componentes de un Expediente Electrónico?

a) Documentos electrónicos, Firma del documento electrónico y Metadatos del documento electrónico.
b) Documentos electrónicos, Índice electrónico, Firma del documento electrónico y Metadatos del documento electrónico.
c) Documentos electrónicos, Índice electrónico, Firma del índice electrónico y Metadatos del expediente electrónico.

68. Según la NTI de Expediente Electrónico, ¿cuáles son las fases del ciclo de vida de un Expediente Electrónico?

a) Apertura, Tramitación, Consolidación y Cierre.
b) Apertura, Tramitación, Conservación y Selección.
c) Apertura, Tramitación, Conservación y Finalización.

69. Según la NTI de Expediente Electrónico, ¿cuál de los siguientes NO es un metadato mínimo obligatorio de un Expediente Electrónico?

a) Origen.
b) Clasificación.
c) Interesado.

70. Según la NTI de Expediente Electrónico, ¿cuál de los siguientes datos debe aparecer obligatoriamente dentro de un índice electrónico de un expediente electrónico objeto de intercambio?

a) Fecha de incorporación de cada documento al expediente.
b) Orden del documento dentro del expediente.
c) Huella digital de cada documento electrónico.

71. ¿Qué elemento NO está incluido en la NTI de Política de Gestión de Documentos Electrónicos?

a) Procesos horizontales de gestión de documentos electrónicos.
b) Especificaciones sobre requisitos funcionales de software para gestión de documentos electrónicos.
c) Principios necesarios para la gestión de documentos electrónicos.

72. Según la NTI de Gestión de Política de gestión de documentos electrónicos, ¿cuál de los siguientes componentes NO forma parte de un Sistema de Gestión de Documentos Electrónicos?

a) Los recursos, tanto humanos como materiales, necesarios para el correcto funcionamiento del sistema.
b) Un programa de tratamiento para la gestión de documentos electrónicos.
c) Una política de firma electrónica de documentos electrónicos.

73. Según la NTI de Gestión de Política de gestión de documentos electrónicos, ¿quién aprobará la Política de Gestión de Documentos Electrónicos?

a) La alta dirección.
b) Los responsables de procesos de gestión.
c) Los responsables de la planificación, implantación y administración del programa de tratamiento de documentos.

74. ¿En qué proceso de gestión de documentos electrónicos de una organización se incluye el tratamiento de los metadatos mínimos obligatorios definidos en la NTI de Documento Electrónico?

a) Clasificación de documentos.
b) Captura de documentos.
c) Descripción de documentos.

75. ¿Cuál de los siguientes algoritmos de cifrado es asimétrico?

a) AES.
b) RSA.
c) DES.

76. En el protocolo IP, ¿cuántos bits se dedican para identificar el host en una red de clase B?

a) 8.
b) 16.
c) 24.

77. Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿cuál de los siguientes NO es un accidente de trabajo?

a) El que sufra el trabajador o la trabajadora al ir o al volver del lugar de trabajo
b) Los ocurridos durante el desempeño de las funciones sindicales
c) Los acaecidos en actos de salvamento y en otros de naturaleza análoga, cuando unos y otros no tengan conexión con el trabajo

78. Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, la posibilidad de que un trabajador o trabajadora sufra un determinado daño derivado del trabajo es:

a) Un riesgo laboral
b) Daño derivado del trabajo
c) Accidente de trabajo

79. Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿cuál de las siguientes es una obligación del trabajador/a recogida en la Ley de Prevención de Riesgos Laborales?:

a) Vigilancia de la salud
b) Utilizar correctamente los medios y equipos de protección
c) Analizar las posibles situaciones de emergencia

80. Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, el incumplimiento por parte del empresario/a de sus obligaciones en materia de prevención de riesgos laborales dará lugar a responsabilidades:

a) Administrativas y penales, pero en ningún caso civiles
b) Administrativas y civiles, pero en ningún caso penales
c) Administrativas, así como en su caso, civiles y penales

81. Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿cuáles son los tres pasos del código PAS?

a) Proteger, ayudar, socorrer
b) Proteger, avisar, socorrer
c) Proteger, animal, socorrer

82. Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿a qué término corresponde la siguiente definición?

"Se define como un patrón de reacciones emocionales, cognitivas, fisiológicas y de comportamiento a ciertos aspectos adversos o nocivos del contenido del trabajo, organización del trabajo y el medio ambiente de trabajo. Es un estado que se caracteriza por altos niveles de excitación y de respuesta y la frecuente sensación de no poder afrontarlos"

a) Estrés laboral
b) Insatisfacción laboral
c) Acoso laboral

83. Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿cuál de los siguientes elementos NO forma parte del "triángulo del fuego"?

a) Combustible
b) Comburente
c) Reacción en cadena

84. Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, respecto a los colores de seguridad en la señalización óptica, ¿qué significa el color azul?

a) Situación de seguridad
b) Señal de prohibición
c) Señal de obligación

85. El II Plan de Igualdad de la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda tiene entre sus objetivos principales:

a) Garantizar que las contrataciones no se basen en estereotipos acerca de aptitudes o características de las personas de determinados sexos, raza, edad, condición social, convicciones o ideales.
b) Conseguir una representación desequilibrada de las mujeres y hombres en el ámbito de la empresa: en grupos profesionales, ocupaciones y en la estructura directiva de la empresa.
c) Evitar la formación para el desarrollo profesional.

86. Según el XI Convenio Colectivo de la FNMT-RCM, el periodo de prueba para el personal técnico con requerimiento de titulación de grado medio, superior o asimilado será de:

a) 2 meses
b) 4 meses
c) 6 meses