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.

OE: 25/23

UNA plaza de INGENIERO DE PROYECTOS (Nivel 14) en el DEPARTAMENTO DE CERES.

AVISO

Estudiadas las solicitudes recibidas, no se estiman las impugnaciones a las preguntas de la prueba teórica 2, 12, 18 y 25 por considerarse correctas por el Tribunal:

- **Pregunta 2 - respuesta correcta A) – no se anula.**

Indique cuál de los siguientes procesos y procedimientos para la validación de la propiedad o el control del dominio por parte del solicitante NO está permitido para la expedición de certificados electrónicos de autenticación web.

a) Validación del Solicitante como contacto de Dominio
b) Correo electrónico, fax, sms o correo postal para el contacto de Dominio
c) Cambio de DNS

Expone:

- Pregunta nº 2: La pregunta está mal formulada en cuanto a que no especifica que el certificado de servidor tenga que ser de tipo EV por lo que no aplica la restricción que impide la respuesta a. Por tanto la pregunta tiene varias respuestas válidas y debería ser anulada.

Respuesta:

Los requisitos básicos para la emisión y gestión de certificados SSL/TLS de confianza pública son normas comunes para la emisión de certificados SSL/TLS más allá de los certificados de tipo EV e incluye todos los certificados validados por dominio (DV) y validados por organización (OV).

En la sección 3.2.2.4 de la guía Baseline Requirements del CAB Forum (en adelante BRG) se exponen los procesos y procedimientos permitidos para validar que el Solicitante tiene la propiedad o control del dominio. Dentro de todos los múltiples procesos enumerados, según la sección 3.2.2.4.1 de la BRG, el procedimiento indicado en la respuesta a) ha sido retirado y NO debe ser usado.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

- **Pregunta 12.- respuesta correcta C) – no se anula**

Cuando se trata de la identificación del solicitante, ¿en qué se diferencian fundamentalmente un certificado OV (Organizational Validation) y un certificado EV (Extended Validation)?

a) La identificación no es parte del proceso de emisión de certificados.
b) La identificación en ambos casos sigue el mismo proceso.
c) La identificación en un certificado EV es más rigurosa que en un certificado OV

Expone:

- Pregunta nº 12: el temario indicado en la convocatoria (en particular los documentos del CAB Forum) no detalla los requerimientos en cuanto a la identificación del solicitante en el caso de certificados OV. Por tanto NO es posible responder a la pregunta con el temario de la convocatoria. Por este motivo debería ser anulada.

Respuesta:

Toda la información necesaria para contestar esta pregunta se encuentra distribuida en el temario de la convocatoria. En concreto en:

- Baseline Requirements;
- EV SSL Certificate Guidelines del CAB Forum; y
- ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

En la sección 7.1.2.7.1 Subcriber Certificate Types de la guía de Requisitos Básicos de CabForum, se mencionan los tipos de certificados que pueden ser emitidos (Domain Validated (DV), Individual Validated (IV), Organization Validated (OV) y Extended Validation (EV))

7.1.2.7.1 Subscriber Certificate Types

There are four types of Subscriber Certificates that may be issued, which vary based on the amount of Subject Information that is included. Each of these certificate types shares a common profile, with three exceptions: the `subject` name fields that may occur, how those fields are validated, and the contents of the `certificatePolicies` extension.

Type	Description
Domain Validated (DV)	See Section 7.1.2.7.2
Individual Validated (IV)	See Section 7.1.2.7.3
Organization Validated (OV)	See Section 7.1.2.7.4
Extended Validation (EV)	See Section 7.1.2.7.5

Note: Although each Subscriber Certificate type varies in Subject Information, all Certificates provide the same level of assurance of the device identity (domain name and/or IP address).

En las secciones 7.1.2.7.4 y 7.1.2.7.5 se especifican los atributos que deben contener el campo subject para los certificados OV y EV respectivamente.

Las BRG exigen que las Autoridades de Certificación (CA) verifiquen todos los contenidos de un certificado, excepto la información contenida en el campo de unidad organizativa. Para la emisión de ambos certificados, las CA tienen que verificar el propietario del dominio, así como varios datos relacionados con la organización, como el nombre, el tipo, el estado y la dirección física. Además de confirmar la autenticidad de la solicitud del certificado.

Lo que diferencia a los certificados EV, es que su emisión exige pasos de validación adicionales para obtenerlos, tal y como se indica en la "guía de emisión y gestión de certificados de validación extendida" del CAB Forum (https://cabforum.org/extended-validation/) y se indica en la sección de 7.1.2.7.5 Extended Validation de la BRG.

7.1.2.7.5 Extended Validation

For a Subscriber Certificate to be Extended Validation, it MUST comply with the Certificate Profile specified in the then-current version of the Guidelines for the Issuance and Management of Extended Validation Certificates. In addition, it MUST meet the following profile:

Field	Requirements
`subject`	See Guidelines for the Issuance and Management of Extended Validation Certificates, Section 9.2.
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.1` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6 and the Guidelines for the Issuance and Management of Extended Validation Certificates.

- **Pregunta 18 – respuesta correcta B) - No se anula.**

De acuerdo a la norma ETSI EN 319 401, un parche de seguridad debe:

a) Aplicarse inmediatamente.
b) Aplicarse en un tiempo razonable tras estar disponible.
c) Aplicarse inmediatamente y documentarse en el caso de que introduzca otra vulnerabilidad de seguridad.

Expone:

- Pregunta nº 18: la norma es muy clara (REQ 7.7-09) los parches se deben aplicar si están disponibles Y no introducen otras vulnerabilidades,etc. (Es un Y no un O) Por tanto la respuesta b NO es cierta al estar incompleta. Una parche de de seguridad no se puede instalar así como así por mucho que haya pasado un tiempo razonable. Por tanto ninguna respuesta es válida y la pregunta debería anularse.

Explicación:

La norma dicta:

- **REQ-7.7-09:** The TSP shall specify and apply procedures for ensuring that:
  a) security patches are applied within a reasonable time after they come available;
  b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
  c) the reasons for not applying any security patches are documented.

La respuesta marcada como correcta (b) es la única de las respuestas declarada cómo uno de los pasos que se deben cumplir al instalar un parche de seguridad. Efectivamente no es la única condición, pero tampoco en la pregunta se especifica que sea una condición necesaria y suficiente.

- **Pregunta 25 – respuesta correcta B) - No se anula.**

Bajo el reglamento EN 319 421 v1.2.1 una TSA operará sus TSUs:

a) Siguiendo obligatoriamente la política BTSP (itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1))
b) Cumpliendo la política BTSP o restringiéndola adicionalmente y declarándolo en sus estamentos
c) Siguiendo cualquier política siempre y cuando la declare en los estamentos de la TSA

Expone:

La respuesta "c" también es correcta puesto que la lista contiene los servicios que proveen los TSP y su status. Por tanto todos aquellos servicios con el estado correspondiente deben estar activos y en funcionamiento.
Por tanto la respuesta contiene más de una respuesta correcta y debería ser anulada

Explicación:

El enunciado expone que la TSA operar bajo el reglamento EN 319 421 v.1.2.1, en cuyo apartado 5.1 Requerimiento Generales se indica:

5.1 General requirements

The policy requirements are defined in the present document in terms of a time-stamp policy. The present document specifies one time-stamp policy: a Best practices Time-Stamp Policy (BTSP) for TSAs issuing time-stamps, supported by public key certificates, with an accuracy of 1 second or better.

OVR-5.1-01: A TSA may define its own policy which enhances a policy defined in the present document.

OVR-5.1-02 [CONDITIONAL]: If the TSA defines its own policy it shall incorporate or further constrain the requirements identified in the present document.

OVR-5.1-03 [CONDITIONAL]: If an accuracy of better than 1 second is provided by the TSA then the accuracy shall be indicated in the TSA's disclosure statement (see clause 6.3) and in each time-stamp issued to an accuracy of better than 1 second.

La respuesta a) no es correcta, la norma no obliga al cumplimiento BTSP, c) no es correcta, dado que cualquier política no es válida, aunque se declare. Si una TSA define su propia política deberá incluir o mejorar los requisitos indicados en la norma EN 319 421. Por lo tanto, solo la respuesta b) es correcta.

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.

Se mantienen por tanto los resultados de la prueba teórica eliminatoria publicados el 19 de diciembre de 2023.

Corregidas las pruebas prácticas de los candidatos que han superado la prueba teórica eliminatoria, se han obtenido los siguientes resultados:

Nº Justificante	**Apellidos, Nombre**	**Práctica no eliminatoria (40%)**
7900010966723	IGEÑO RODRIGUEZ, DAVID	7,350
7900011017150	GARCIA ESCARTIN, DAVID	5,790

Se establece plazo de presentación de solicitud de revisión de la prueba práctica de aquellas personas a las que se ha corregido los días 10, 11 y 12 de enero de 2024. Los escritos deberán presentarse con DNI electrónico o certificado digital a través del Registro electrónico común de la Administración General del Estado indicando la referencia "OE 25/23": https://rec.redsara.es/registro/action/are/acceso.do

Se convoca a las personas que han superado la prueba teórica a la realización de la **prueba de inglés eliminatoria** el próximo **22 de enero de 2024** a las **9:30 horas** en el **Centro de Formación de la FNMT**.

Madrid, a la fecha de la firma electrónica
LA SECRETARIA DEL TRIBUNAL