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

Realizada la prueba teórica eliminatoria se han obtenido los resultados que se adjuntan.

Se establece plazo de presentación de impugnaciones los días 20, 21 y 22 de diciembre de 2023. Las impugnaciones 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 publican las preguntas y la plantilla de corrección de la prueba teórica eliminatoria.

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

OE 25/23 Ingeniero de Proyectos

Prueba teórica eliminatoria

REGISTRO	APELLIDOS, NOMBRE	NOTA
7900010875583	MAZUECOS VELAZQUEZ, BERTA	2,647
7900010952452	SANCHEZ BARRENA, JORGE	1,324
7900010965271	GARROTE FRANCO, JOSÉ MIGUEL	1,471
7900010966723	IGEÑO RODRIGUEZ, DAVID	5,980
7900010999133	SANCHEZ PASCUAL, ALBERTO	1,029
7900011017150	GARCIA ESCARTIN, DAVID	6,961
7900011017604	SOMOLINOS CERRADA, JESUS	4,510
7900011018480	LAJUSTICIA AISA, ANGEL	4,069
790001338551023615	RODRIGUEZ ROLDAN, CARLOS	4,069

OE 25/23

INGENIERO DE PROYECTOS

PRUEBA TEÓRICA ELIMINATORIA

---

1. **De acuerdo a las especificaciones de Baseline Requirements (BRG) de CAB Forum, la Declaración de Practicas de Confianza deberán estar estructurada de acuerdo con:**
   a) RFC 5280
   b) RFC 3647
   c) RFC 6960
2. **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
3. **Según las especificaciones de Baseline Requirements (BRG), antes de emplear cualquier fuente de información como una fuente confiable, la Autoridad de Certificación(AC) DEBERÁ evaluar la fuente para conocer su fiabilidad, precisión y resistencia a alteraciones o falsificaciones. Durante su evaluación, la AC NO DEBERÁ considerar:**
   a) La antigüedad de la información suministrada.
   b) La accesibilidad pública de la disponibilidad de información.
   c) Las bases de datos mantenidas por la AC con el objetivo de recopilar información para la validación de la identidad.
4. **Según las especificaciones de Baseline Requirements (BRG), el informe de auditoría entre otra información, DEBE contener:**
   a) Nombre de organización auditada; la huella digital SHA-256 de todos los certificados de AC root y de AC subordinada, sin incluir los certificados cruzados, que están dentro del alcance de la auditoría; la fecha de inicio y de finalización del periodo auditado
   b) Nombre de organización auditada; la huella digital SHA-1 de todos los certificados de AC root y de AC subordinada, incluyendo certificados cruzados, que están dentro del alcance de la auditoría; la fecha de inicio y de finalización del periodo auditado
   c) Nombre de organización auditada; La huella digital SHA-256 de todos los certificados de AC root y de AC subordinada, incluyendo certificados cruzados, que están dentro del alcance de la auditoría; la fecha de inicio y de finalización del periodo auditado
5. **Según las especificaciones de Baseline Requirements (BRG), si la Autoridad de Certificación(AC) obtiene evidencias que indican que la clave privada del suscritor, correspondiente a la clave pública en el certificado ha sufrido un compromiso, DEBERÁ:**
   a) Revocar el certificado de suscritor en 48 horas
   b) Revocar el certificado de suscritor en 24 horas
   c) Revocar el certificado de suscritor en 7 días.
6. **Según las especificaciones de Baseline Requirements (BRG), si la Autoridad de Certificación(AC) obtiene evidencias que indican que el certificado de una de sus AC subordinado ha sido incorrectamente usado, DEBERÁ:**
   a) Revocar el certificado de la AC Subordinada en 48 horas
   b) Revocar el certificado de la AC Subordinada en 24 horas
   c) Revocar el certificado de la AC Subordinada en 7 días

7. **Según la política de Mozilla Root Store, todas las Políticas de Certificación (PC) y Declaración de Prácticas de Certificación (DPC) DEBEN:**
   a) Ser revisadas, solo si se es necesario realizar cambios por la publicación de nuevos requisitos de S/MIME o TLS. Se incrementará el número de versión y añadirá una entrada fechada en el registro de cambios.
   b) Ser revisadas al menos una vez cada 365 días. Si no hay cambios, no se incrementará el número de versión, ni añadirá una entrada fechada en el registro de cambios.
   c) Ser revisadas, según sea necesario al menos una vez cada 365 días. Se incrementará el número de versión y añadirá una entrada fechada en el registro de cambios, incluso si no se realizan otros cambios en el documento.

8. **¿Qué es el CCADB?**
   a) Base de Datos Común de Autoridades de Certificación creado por los navegadores, un repositorio de datos de información sobre certificados y Autoridades de Certificación Europeas
   b) Base de Datos Común de Autoridades de Certificación creado por el Organismo Supervisor Europeo, un repositorio de datos de información sobre certificados y Autoridades de Certificación Europeas
   c) Base de Datos Común de Autoridades de Certificación, un repositorio de datos de información sobre certificados y Autoridades de Certificación aceptados en los navegadores Web

9. **Indique la INCORRECTA. Un certificado TLS de entidad final puede ser revocado por el siguiente motivo:**
   a) keyCompromise
   b) certificateHold
   c) unspecified

10. **Según la Política y Prácticas de Certificación Particulares de certificados de personas físicas de la AC FNMT Usuarios, ¿Con que frecuencia se generan las CRLs de la Autoridad de Certificados?**
   a) Se emiten al menos cada 12 horas, o cuando se produce una revocación y tienen un periodo de validez de 24 horas.
   b) Se emiten cada 6 meses, o cuando se produce una revocación y tienen un periodo de validez de 6 meses.
   c) Se emiten al menos cada 24 horas, o cuando se produce una revocación y tienen un periodo de validez de 48 horas.

11. **¿Cuál de las siguientes respuestas NO es obligación de la Autoridad de Registro?**
   a) Validar la identidad del solicitante antes de emitir un certificado.
   b) Mantener la confidencialidad de la información del solicitante.
   c) Generar claves criptográficas para los certificados.

12. **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.

13. **El periodo de vigencia de los certificados cualificados:**
   a) No será superior a 5 años
   b) No será superior a 4 años
   c) Será establecido libremente por los Prestadores de Servicios de Confianza, no habiéndose establecido limitación alguna en la duración máxima de los mismos

14. **Dentro de los servicios proporcionado por un prestador de servicios de confianza, señala la afirmación que NO es correcta:**
    a) El servicio de registro verifica la identidad y, en su caso, los atributos específicos de un sujeto.
    b) El servicio de generación de certificados: difunde los certificados a los sujetos y, si éstos dan su consentimiento los pone a disposición de las partes usuarias. Este servicio también pone a disposición los términos y condiciones de la CA atributos verificados por el servicio de registro.
    c) El servicio de estado de revocación proporciona información sobre el estado de revocación de certificados a las partes usuarias basándose en listas de revocación de certificados o en un servicio en tiempo real que proporciona información sobre el estado de los certificados de forma individual.
15. **De acuerdo a la norma ETSI EN 319 401, ¿qué servicio no caería bajo su definición de servicio de confianza (trust service)?**
    a) creación, verificación y validación de firmas digitales y sus certificados asociados.
    b) creación, verificación y validación de una transacción financiera.
    c) creación, verificación y validación de certificados de autenticación web.
16. **De acuerdo a la norma ETSI EN 319 401, un TSP (Trust Service Provider), ¿con qué plazo debe notificar una quiebra de seguridad o de integridad que tenga un impacto significativo en el servicio?**
    a) Tan pronto se tenga seguridad que está solucionado.
    b) En un plazo de 24 horas desde que se tenga constancia de la brecha.
    c) En un plazo de 48 horas tras certificar que la quiebra está solucionada.
17. **De acuerdo a la norma ETSI EN 319 401, ¿con qué periodicidad mínima un TSP debe programar un test de penetración sobre sus sistemas?**
    a) No es necesario si el TSP está certificado, y no se ha detectado nada en los tests de vulnerabilidad.
    b) Una vez al año.
    c) Según establezca el TSP y quedando registrado en la CPS (Certification Practice Statement).
18. **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.
19. **De acuerdo a la norma ETSI EN 319 411-1 una CPS (Certification Practice Statement):**
    a) Describe cómo opera un TSP sus servicios.
    b) Describe un certificado en términos de calidad, aplicabilidad, perfil del certificado.
    c) Es un documento opcional para un TSP, donde se establecen una relación de buenas prácticas.
20. **Según la norma ETSI EN 319 411-1 la política Extended Validation Certificate Policy (EVCP) tiene como base la política:**
    a) NCP
    b) LCP
    c) QTSA
21. **Según la norma ETSI EN 319 411-1, ¿cuál no sería un servicio propio de la certificación?**
    a) Servicio de registro.
    b) Servicio de firma digital.
    c) Servicio de generación de certificado.
22. **Según la norma ETSI EN 319 411-1, ¿Qué servicio de consulta de estado certificado no está contemplado?**
    a) LDAP
    b) OCSP
    c) CRL

23. **Según la norma ETSI EN 319 411-1, ¿un TSP puede generar y custodiar la clave privada de un sujeto?**
    a) En ningún caso.
    b) Sí, pero garantizando que solo el sujeto tiene control y uso de ella.
    c) Es una opción que se le deba dar siempre al usuario en la fase de registro.

24. **¿De qué norma emana la definición de los certificados declarados en la norma ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates?**
    a) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.
    b) Reglamento (UE) n ° 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) Reglamento (UE) 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

25. **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

26. **Bajo el reglamento EN 319 421 v1.2.1 un sello de tiempo emitido por una TSU:**
    a) Incluirá el tiempo procedente de una fuente de tiempo sincronizada con el UTC.
    b) Estará firmado con la clave del servidor SSL que presta el servicio de dicha TSU.
    c) Podrá incluir un tiempo des-sincronizado si su fuente está des-sincronizada, pero deberá especificarlo como parte de la respuesta.

27. **De acuerdo al manual "GUÍA PARA LA ELABORACIÓN DE PROYECTOS" indicado en el temario de la convocatoria, ¿cuáles son las fases del ciclo de vida de un proyecto?**
    a) Planificación, ejecución y entrega del proyecto.
    b) Diseño, planificación, ejecución, seguimiento y control, evaluación y cierre del proyecto.
    c) Toma de requisitos, planificación, ejecución y fin del proyecto.

28. **De acuerdo al manual "GUÍA PARA LA ELABORACIÓN DE PROYECTOS" indicado en el temario de la convocatoria, la gestión de riesgos en un proyecto caería dentro de la fase de:**
    a) Planificación.
    b) Diseño.
    c) Ejecución.

29. **La norma, ETSI TS 119 612: Electronic Signatures and Infrastructures (ESI);Trusted Lists. Establece:**
    a) Los requisitos para la certificación como Trust Service Provider.
    b) Una plantilla común para los Trusted List Scheme Operator para proveer el estado de los servicios prestados por un Trust Service Provider.
    c) La lista de los servicios que deben proveer los Trust Service Providerers dentro del marco de la Unión Europea.

30. **Según la ETSI TS 119 431-1 V1.2.1, Policy and security requirements for Trust Service Providers; Part 1: TSP service components operating a remote QSCD/SCDev. ¿Cuál de las siguientes políticas, SSASC, es menos restrictiva?**
    a) LSCP
    b) NSCP
    c) EUSCP

31. **Seleccione la afirmación CORRECTA respecto a la expedición de certificados electrónicos cualificados y los métodos de identificación remota del solicitante:**
    a) Es necesario que el proceso de identificación remota por vídeo se realice de forma asistida, con la mediación síncrona de un operador que verifique la autenticidad, vigencia e integridad de los documentos de identificación aportados.
    b) Sólo se podrá emitir mediante identificación remota certificados electrónicos no cualificados.
    c) Es posible que la acreditación se realice mediante un proceso de identificación remota por vídeo de forma no asistida, sin necesidad de interacción en línea entre un operador y el solicitante.

32. **¿Cuándo podrá empezar a operar un prestador cualificado de servicios de confianza sus procedimientos basados en identificación remota por vídeo?**
    a) Cuando notifique su actividad mediante la solicitud correspondiente a la Secretaría de Estado de Digitalización e Inteligencia Artificial
    b) En un periodo inferior a 6 meses desde que el prestador remita solicitud para la puesta en operación de procedimientos de identificación remota por vídeo a la Secretaría de Estado de Digitalización e Inteligencia Artificial, siempre y cuando reciba notificación de la resolución favorable del órgano supervisor
    c) Cuando el organismo de evaluación emita informe favorable de cómo cumple el prestador los requisitos definidos en la Orden ETD/465/2021, por la que se regulan los métodos de identificación remota por vídeo

33. **El prestador cualificado de servicios electrónicos de confianza dispondrá de un modelo de gestión continua del riesgo que incluirá un análisis de riesgos especifico que se revisará...**
    a) Al menos con una periodicidad mínima anual.
    b) Al menos cada 6 meses, y, en todo caso, siempre que se produzca un cambio en el sistema, en los procedimientos organizativos, en el estado de la tecnología, o en cualquier otro aspecto que pudiera influir en el perfil de riesgo del procedimiento de identificación.
    c) Al menos de forma bianual, y, en todo caso, siempre que se produzca un cambio en el sistema, en los procedimientos organizativos, en el estado de la tecnología, o en cualquier otro aspecto que pudiera influir en el perfil de riesgo del procedimiento de identificación.

34. **El prestador cualificado de servicios electrónicos de confianza que ofrezca procedimientos basados en identificación remota por video …**
    a) Adoptará exclusivamente las medidas técnicas y organizativas indicadas en la Orden ETD/465/2021, por la que se regulan los métodos de identificación remota por vídeo
    b) Podrá adoptar medidas técnicas y organizativas adicionales a las indicadas en la Orden ETD/465/2021, cuando el resultado del análisis de riesgos efectuado así lo requiera
    c) Notificará inmediatamente al órgano supervisor, y en cualquier caso antes de 72 horas desde su conocimiento, cualquier violación de la seguridad o pérdida de integridad que tenga impacto en el servicio

35. **De acuerdo a las Condiciones generales del proceso de identificación por video acreditación establecidas en la Orden ETD/465/2021, indique en cuál de estas circunstancias el proceso de identificación se podría considerar válido.**
    a) La calidad de la imagen o el sonido impidan o dificulten verificar la autenticidad e integridad del documento de identificación y la correspondencia entre el titular del documento y el solicitante.
    b) Existan indicios de que la transmisión de vídeo no se ha realizado en tiempo real o de que el proceso no se ha realizado en unidad de acto.
    c) Existan indicios de que el solicitante está siendo ayudado o tenga asistencia de otra persona.

36. **Con respecto a los Requisitos de la grabación y de conservación de pruebas en un proceso de identificación por video acreditación...**
    a) Se conservará una copia de la grabación del vídeo durante un periodo mínimo de tiempo de 10 años desde la extinción de la vigencia del certificado obtenido por este medio.
    b) Se conservarán, por un periodo mínimo de tiempo de 5 años, fotos o capturas de pantalla del solicitante y del documento de identidad utilizado, en las que serán claramente reconocibles tanto la persona como el anverso y el reverso del documento de identidad.
    c) Se conservará, por un periodo mínimo de tiempo de 15 años, el resultado automático de la verificación realizada por la aplicación, así como la evaluación y observaciones realizadas por el operador junto a su decisión de aprobación o rechazo de la identificación.

37. **Las Administraciones Públicas NO podrán utilizar el siguiente sistema para su identificación electrónica y para garantizar el origen e integridad de los documentos electrónicos:**
    a) Sello electrónico basado en un certificado electrónico cualificado y que reúna los requisitos exigidos por la legislación de firma electrónica
    b) Firma electrónica del personal al servicio de las Administraciones Públicas
    c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital

38. **Seleccione para qué NO se podría usar un sello electrónico basado en un certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica de acuerdo al Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos:**
    a) Identificación de las Administraciones públicas para la actuación administrativa automatizada
    b) Identificación de las sedes electrónicas y de las sedes electrónicas asociadas
    c) Para garantizar el origen e integridad de los documentos electrónicos

39. **¿Cuál de los siguientes medios puede ser usado como sistema de firma electrónica para la actuación administrativa automatizada?**
    a) Código seguro de verificación o CSV
    b) Firma electrónica del personal al servicio de las Administraciones Públicas
    c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital

40. **Las personas interesadas en el procedimiento NO podrán utilizar el siguiente sistema para su identificación electrónica:**
    a) Código seguro de verificación o CSV
    b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza»
    c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital

41. **Según la RFC 5280 - Internet X.509 Public Key Infrastructure, ¿cuál es el período de validez máximo de un certificado X.509?**
    a) 4 años
    b) 5 años
    c) Esta RFC no define el periodo de validez máximo de un certificado X.509

42. **¿Cuál es el propósito de una CRL?**
    a) Listar los certificados que han sido revocados antes de su fecha de expiración
    b) Listar los certificados que han sido emitidos por una CA específica
    c) Listar los certificados que han sido utilizados para realizar transacciones fraudulentas

43. **Un certificado X.509 contiene el siguiente campo: Key Usage: digitalSignature, keyEncipherment. ¿Qué significa esto?**
    a) El certificado puede utilizarse para verificar firmas digitales y cifrar claves.
    b) El certificado puede utilizarse para firmar digitalmente documentos, pero no para cifrar claves.
    c) El certificado puede utilizarse para cifrar claves, pero no para verificar firmas digitales.

44. **Según la RFC 5280 - Internet X.509 Public Key Infrastructure, ¿Qué es una cadena de confianza (o 'certification path')?**
    a) Una secuencia de certificados que comienza con un certificado de raíz y termina con el certificado que se está verificando
    b) La ubicación de un certificado electrónico en un sistema de ficheros
    c) Hace referencia al establecimiento de una sesión mutuamente autenticada en la que se emplea un certificado de servidor web y un certificado de cliente

45. **El Suscriptor de un Certificado puede ser una entidad diferente de la figura de Firmante cuando hay una relación de representación o pertenencia a una Organización. Seleccione la afirmación CORRECTA.**
    a) El firmante de un Certificado de Empleado Público es la persona física que mantiene bajo su uso exclusivo los Datos de creación de firma asociados a dicho Certificado
    b) El firmante de un Certificado de Empleado Público es la entidad para la que se ha emitido dicho Certificado
    c) El firmante de un Certificado de Firma Centralizada para Empleado Público es la entidad que mantiene bajo su exclusivo control los Datos de creación de firma asociados a dicho Certificado

46. **¿En qué circunstancias es posible solicitar a la Autoridad de Certificación la modificación de un certificado emitido?**
    a) Inexactitudes en los datos aportados por el Solicitante para la obtención del Certificado, o alteración de los datos aportados para la obtención del Certificado.
    b) Modificación de las circunstancias verificadas para la expedición del Certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
    c) No es posible realizar modificaciones de los certificados expedidos. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo Certificado.

47. **Seleccione la afirmación CORRECTA:**
    a) Un Certificado con Seudónimo, es el Certificado de persona física de la AC FNMT Usuarios que vincula un seudónimo otorgado por la DGP a la persona que realiza labores que puedan comprometer la seguridad nacional
    b) Es obligaciones de la Autoridad de Certificación comprobar que el interesado en solicitar la emisión de un Certificado posee el control de la Clave Privada que constituirá, una vez emitido el Certificado, los Datos de creación de Firma correspondientes a los de Datos de verificación de Firma que constarán en el Certificado, y comprobar su complementariedad
    c) La FNMT-RCM expedirá el Certificado de Firma Electrónica sin necesidad de que el peticionario comparezca ante una Oficina de Registro si, en el proceso de solicitud de dicho Certificado, el Solicitante se identifica utilizando un Certificado cualificado emitido por cualquier prestador cualificado de servicios de confianza que cumpla los requisitos establecidos en el anexo I del Reglamento UE 910/2014 del Parlamento Europeo

48. **De acuerdo con el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, indique la afirmación errónea con respecto a los niveles de auditoría que se realizan a los sistemas de información:**
    a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría.
    b) En sistemas de información de categoría MEDIA bastará una autoevaluación realizada por el mismo personal que administra el sistema de información o en quien éste delegue.
    c) Los informes de auditoría de los sistemas de información de categoría ALTA serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema.

49. **De acuerdo con el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, en la Medida de Seguridad de "Segregación de funciones y tareas" señale la opción INCORRECTA:**
    a) Las capacidades de desarrollo y operación nunca recaerán en la misma persona.
    b) Siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema.
    c) La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

50. **De acuerdo con el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, a fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados, se tendrán en cuenta las siguientes dimensiones de la seguridad:**
    a) Autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad.
    b) Atomicidad, consistencia, integridad, durabilidad y trazabilidad.
    c) Accesibilidad, consistencia, identidad, disponibilidad y transparencia.

51. **De acuerdo con el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, en lo que se refiere al ámbito de aplicación del real decreto señale la opción INCORRECTA:**
    a) Es de aplicación a todo el sector público.
    b) Se aplica a los sistemas de información de las entidades del sector privado cuando presten servicios o provean soluciones a las entidades del sector público para el ejercicio por éstas de sus competencias.
    c) No será de aplicación a los sistemas que tratan información clasificada, puesto que se rigen por la Ley 9/1968, de 5 de abril, de Secretos Oficiales.

52. **Indique cuál de los siguientes NO es un grupo de Medidas de Seguridad de los establecidos en el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad:**
    a) Marco operacional.
    b) Marco de gestión.
    c) Medidas de protección.

53. **De acuerdo con el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, un sistema de información será categorizado como de categoría MEDIA:**
    a) Si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO y ninguna alcanza un nivel de seguridad superior.
    b) Si todas sus dimensiones de seguridad alcanzan el nivel de seguridad MEDIO.
    c) Si la mayoría de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO.

54. **De acuerdo con el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, hay 3 tipos de factores de autenticación. Señale el factor erróneo:**
    a) Algo que se sabe, un secreto.
    b) Algo que identifica, un certificado.
    c) Algo que se es, biometría.

55. **De acuerdo con el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad que se formalizarán en un documento denominado Declaración de Aplicabilidad:**
    a) Firmado por el Responsable de la Seguridad.
    b) Firmado por el Responsable de la Seguridad y el Responsable del Servicio.
    c) Firmado por el Responsable de la Seguridad y el Responsable de la Información.

56. **De acuerdo con la Guía de Seguridad de las TIC CCN-STIC 802, en cuanto a la certificación de la conformidad de los sistemas, indique la opción correcta:**
    a) Los sistemas de categoría Baja pueden someterse a una auditoría formal de certificación de la conformidad, aunque esta posibilidad no es la deseable.
    b) Los sistemas de categoría Media precisarán de una auditoría formal para su certificación de la conformidad al menos cada dos años.
    c) Los sistemas de categoría Alta precisarán de una auditoría formal para su certificación de la conformidad al menos cada año.

57. **Según el Reglamento General de Protección de Datos (UE) 2016/679, en su artículo 37.1, indique la afirmación ERRÓNEA de los supuestos en los que es obligatorio la designación de un Delegado de Protección de Datos:**
    a) El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
    b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.
    c) Las actividades principales del responsable o del encargado consistan en el tratamiento a pequeña escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

58. **Según el Reglamento General de Protección de Datos (UE) 2016/679, indique cuál es una de las funciones que como mínimo tendrá el delegado de protección de datos:**
    a) Elaborar los planes de concienciación y formación del personal que participa en las operaciones de tratamiento.
    b) Ofrecer asesoramiento acerca de la evaluación de impacto relativa a la protección de datos.
    c) Establecer procedimientos y estructuras para tratar las reclamaciones relativas a las infracciones dispuestas en el presente Reglamento.

59. **Según el Reglamento General de Protección de Datos (UE) 2016/679, la mayor sanción impuesta por una infracción será:**
    a) Multa administrativa de hasta 40.000.000€ o, en el caso de empresas, de cuantía equivalente al 6% como máximo del volumen de negocio total anual, lo que resulte mayor en cuantía.
    b) Multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen de negocio total anual, lo que resulte mayor en cuantía.
    c) El RGPD no especifica cuantía para las sanciones, sino que está desarrollado en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

60. **Según el Reglamento General de Protección de Datos (UE) 2016/679, en el momento que se obtengan de un interesado datos personales relativos a él, se le facilitará toda la información indicada en el artículo 13 de dicho reglamento (por ejemplo, los fines del tratamiento a que se destinan los datos personales y el plazo durante el cual se conservarán). La figura encargada de facilitar la información es:**
    a) El encargado del tratamiento.
    b) El responsable del tratamiento.
    c) El delegado de protección de datos.

61. **Según el XI Convenio Colectivo de la FNMT-RCM, la relación numérica de los puestos de trabajo, que, ordenados por grupos profesionales y categorías, son necesarios para atender de modo suficiente las necesidades permanentes y habituales de la FNMT-RCM es:**
    a) La relación del personal.
    b) El catálogo de puestos de trabajo.
    c) La valoración de puestos de trabajo.

62. **Según el III Plan de Igualdad de la FNMT-RCM, en caso de ser necesario negociar otro plan de igualdad, el proceso se iniciará…**
    a) como máximo, dentro de los tres meses anteriores a la finalización de la vigencia del presente.
    b) como mínimo, dentro de los tres meses anteriores a la finalización de la vigencia del presente.
    c) como mínimo, dentro de los cuatro meses anteriores a la finalización de la vigencia del presente.

63. **Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿cuál de las siguientes es la definición de riesgo profesional?**
    a) Es cualquier fuente o situación con capacidad de producir un determinado daño. Éstos pueden ser lesiones, daños a la propiedad, daños al medioambiente o una combinación.
    b) Será la materialización de un determinado peligro que está presente en el medio laboral.
    c) Son el conjunto de enfermedades, patologías o lesiones sufridas por los trabajadores con motivo u ocasión del trabajo.

64. **En la FNMT-RCM, el número de Delegados de Prevención en el centro de trabajo de Madrid es de:**
    a) 6 Delegados elegidos por el Comité de Empresa, de los que cuatro serán miembros de dicho Comité.
    b) 6 Delegados elegidos por el Comité de Empresa, de los que tres serán miembros de dicho Comité.
    c) 3 Delegados, elegidos por y entre el Comité de Empresa.

65. **Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, el Comité de Seguridad y Salud se reunirá:**
    a) Mensualmente y siempre que lo solicite alguna de las representaciones del mismo
    b) Trimestralmente y siempre que lo solicite alguna de las representaciones del mismo
    c) Semestralmente y siempre que lo solicite alguna de las representaciones del mismo

66. **Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿qué actuación hay que realizar en caso de que una persona esté inconsciente como consecuencia de una obstrucción completa de las vías aéreas?**
    a) Maniobra de Heimlich
    b) Maniobra de reanimación cardiopulmonar
    c) No se ha de realizar maniobra alguna si el paciente está inconsciente

67. **Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿cuál de los siguientes focos de ignición es un foco térmico?**
    a) Producción de chispas eléctricas
    b) Roces mecánicos
    c) Fumar o empleo de mecheros

68. **Según el Manual de Prevención de Riesgos Laborales de la FNMT-RCM, ¿qué afirmación NO es correcta respecto a las medidas preventivas relacionadas con el teclado?**
    a) Entre el teclado y el borde de la mesa tiene que haber un espacio mínimo de 10 cm. para apoyar las muñecas.
    b) El teclado no debe ser inclinable ni independiente de la pantalla.
    c) Utilice el ratón tan cerca del teclado como sea posible.

HOJA DE RESPUESTAS CORRECTAS

Código Exámen 2 5 0 2 3

Número de preguntas 0 6 8

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	●	○	○	○	○	○	○	○	○	○	○
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	○	○	○	○	○	○	○	○	○	○	○
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