Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PROCESO DE SELECCIÓN PARA CUBRIR PLAZAS EN REGIMEN DE CONTRATO LABORAL EN LA MODALIDAD DE FIJO

UNA plaza de TÉCNICO DE SEGURIDAD Y AUDITORÍA INFORMÁTICA (Nivel 12) en la DIRECCIÓN DE SISTEMAS DE INFORMACIÓN

AVISO

Realizadas las revisiones de examen solicitadas, y después de haber revisado el Tribunal el ejercicio nº 4 de todas las pruebas prácticas, se han obtenido los siguientes resultados:

DNI	Apellidos, Nombre	Práctico eliminatorio (50%)
50.845.415	ARIAS LOPEZ, FERNANDO	6,27
3.888.470	CARO ALONSO-RODRIGUEZ, ANTONIO JESUS	5,3
50.107.601	COLLADO ESCALANTE, JUAN LUIS	3,83
51.060.749	DEL REY SANCHEZ, JUAN ANGEL	8,6
12.411.214	GARCIA ESCARTIN, DAVID	4,67
2.885.036	GARCIA NAVAS, JAVIER	4,62
50.896.370	GARCIA NUÑEZ, ALEX	9,4
2.631.730	JUAREZ GONZALEZ, MARTA	9,6
51.990.102	PEREZ PEREZ, LIVIA	3,53
72.036.620	PEREZ PEREZ, RAMON	5,31
70.802.345	PRIETO VICENTE, JOSE IGNACIO	NP
25.456.383	PUERTOLAS GARCIA, JOSE IGNACIO	6,16
26.241.361	QUINTANA LORITE, JUAN ANTONIO	7,8
8.933.872	RODRIGUEZ PINILLOS, HUGO MANUEL	9,4
14.608.425	RUEDA LOPEZ, JAVIER	4,83

La pregunta revisada es la siguiente:

EJERCICIO 4

Hoy, del 12 de mayo del 2017, un usuario ha avisado al Centro de Atención a Usuarios (CAU) sobre un comportamiento extraño en su equipo. Un técnico del CAU acude de inmediato al puesto del usuario afectado y confirma que se trata de algún tipo de virus. A continuación, pone sobre alerta al equipo de seguridad.

TÚ eres el técnico de seguridad que recibe la alerta: coges tus herramientas de trabajo y te diriges al puesto del usuario. Una vez allí, observas la siguiente imagen en la pantalla del equipo afectado:

PROCESO DE SELECCIÓN PARA CUBRIR PLAZAS EN REGIMEN DE CONTRATO LABORAL EN LA MODALIDAD DE FIJO

PREGUNTA 1: ¿A qué tipo de malware nos estamos enfrentando y por qué se caracteriza?

PREGUNTA 2: Considerando toda la información del enunciado y la captura de pantalla ¿Sabrías decir a qué malware en concreto corresponde la infección?

PREGUNTA 3: Antes de que puedas actuar sobre el equipo, la FNMT-RCM recibe un aviso del CCN-CERT alertando sobre la amenaza, que se estaría propagando rápidamente en distintos organismos. El CCN-CERT en su aviso recomienda aislar de la red los equipos infectados y solicitan recabar una serie de información de los mismos antes de apagarlos completamente. Una vez obtenida la hora y fecha del sistema y realizado el volcado de memoria, decides continuar el análisis sobre la evidencia volátil. Para ello has elaborado un pequeño checklist basado en la guía "Guía de toma de evidencias en entornos Windows (INCIBE)".
Además, dispones de varias suites de análisis forense en CDs y USBs (Caine, Helix, Kali, etc.) que incluyen todo tipo de herramientas.
Incluye en la Tabla 1 (página siguiente), al menos 5 evidencias que se perderían al apagar el equipo y puedan resultar relevantes a la hora de investigar un incidente, junto con una breve justificación y las herramientas o comandos necesarios para su obtención.
Nota, se puntuará:

- 0,2 puntos por cada evidencia correcta que incluya referencia a herramienta/comandos también correctos.
- 0,1 puntos por cada evidencia correcta sin referencia a herramienta/comandos.
- 0 puntos por cada evidencia incorrecta o que incluya herramientas/comandos incorrectos.

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PROCESO DE SELECCIÓN PARA CUBRIR PLAZAS EN REGIMEN DE CONTRATO LABORAL EN LA MODALIDAD DE FIJO

PREGUNTA 4: Al concluir la investigación se determinó que el origen de la infección fue un correo electrónico no deseado. Incluye a continuación 4 recomendaciones de seguridad relativas al uso seguro del correo electrónico y a la prevención frente a amenazas (spam, phishing, hoax, etc.) que comunicarías al usuario afectado a modo de concienciación.
Nota, se puntuará:

- 0,25 puntos por cada recomendación correcta y debidamente justificada.

Se establece plazo de presentación de alegaciones los días 15, 16, 17, 22 y 23 de abril de 2019 de 9:00 a 14:00 horas en el Registro General de esta FNMT-RCM, advirtiendo a los candidatos que **sólo podrán revisar la pregunta que ha sido modificada**, tal y como figura en las bases de la convocatoria.

Se convoca a los candidatos que han superado la prueba práctica a la **prueba de inglés no eliminatoria** (nivel B1) en próximo martes **7 de mayo de 2019** a las **9:30 horas** en el **Centro de Formación de la FNMT** (C/ Duque de Sesto nº 47).

Madrid, 12 de abril de 2019

EL SECRETARIO DEL TRIBUNAL

FABRICA NACIONAL DE MONEDA Y TIMBRE - DIRECCION DE RECURSOS HUMANOS - SOMETIDA

Fdo.: José Antonio Guarido Esteban