CONVOCATORIA DE PUESTO EN FASE DE COBERTURA EXTERNA

1. IDENTIFICACIÓN DEL PUESTO

Analista Programador de Seguridad de la Información, en la Dirección TIC, cuya misión será reforzar el equipo de Seguridad de la Información para afrontar las crecientes necesidades en esta materia fruto del aumento de leyes y regulaciones aplicables, la proliferación de amenazas de seguridad, el creciente abanico de sistemas y aplicaciones y la implantación de nuevos modelos de desarrollo y despliegue de aplicaciones.

2. DESCRIPCIÓN DE LAS FUNCIONES A DESARROLLAR

Como parte del equipo de Seguridad de la Información, la persona seleccionada participará en la actividad del equipo encargándose de realizar, entre otras, las siguientes tareas:

- Analizar requisitos de seguridad para desarrollos y adquisiciones
- Elaboración de normativa y procedimientos de seguridad
- Definir los requisitos de configuración segura de sistemas y aplicativos
- Detectar anomalías a partir de información registrada
- Responder a incidentes
- Gestionar vulnerabilidades

3. PERFIL DEL PUESTO

3.1. Perfil académico:

Imprescindible:

- Titulación universitaria Nivel MECES 2 o superior, o sus equivalentes en títulos universitarios pre-Bolonia, en materia de Tecnologías de la Información y las Comunicaciones (TIC).
- Nivel B1 de idioma inglés.

Valorable: Se valorará estar en posesión de un título oficial y homologado de Máster y/o cursos de Postgrado en Ciberseguridad o Seguridad de la Información.

3.2. Experiencia y capacitación profesional:

Imprescindible: Experiencia laboral demostrable de al menos 2 años en actividades de Seguridad de la Información, Seguridad TIC o Ciberseguridad.

Valorable:

Se valorará hasta un máximo de 4 años de experiencia como la anterior.

Se valorará la experiencia en:

- Administración de sistemas (Linux RHEL, Windows, Active Directory)
- Administración de equipos de comunicaciones y cortafuegos
- Administración de proxies de navegación web
- Criptografía aplicada (PKI, uso de OpenSSL, keytool, certutil, etc.)
- Programación de scripts (al menos Python, sh y PowerShell)
- SIEM
- Análisis de protocolos de comunicaciones (Wireshark o similares)
- Elaboración de indicadores de Seguridad de la Información

3.3. Otros conocimientos específicos valorables:

Se valorará estar en posesión de alguna de las siguientes certificaciones profesionales en vigor:

- ISC2 CISSP
- ISACA CISM
- ISO 27001 Auditor o Implementer
- EC Council CEH
- SANS GCIH
- SANS GPEN
- Offensive Security OSCP

Se valorará el conocimiento de alguna de las siguientes materias:

- Gestión de proyectos
- SCRUM

- Sistemas de Gestión de Seguridad de la Información
- Esquema Nacional de Seguridad
- Seguridad en Microsoft Exchange
- Seguridad en Office365
- Seguridad en plataformas móviles (Android, iOS).

3.4. Perfil y competencias profesionales

- Pensamiento analítico
- Mejora continua y orientación al cambio.
- Manejo de conflictos.
- Trabajo en equipo.

4. ACREDITACIÓN DE REQUISITOS Y MÉRITOS VALORABLES

- Los títulos deberán estar acreditados mediante certificados oficiales o diplomas.
- Los cursos deberán estar acreditados mediante títulos o diplomas. Cuando en el título o diploma no conste el nivel del curso, éste será considerado como de nivel básico.
- La experiencia deberá estar acreditada mediante informe de vida laboral, además de los contratos y/o certificados acreditativos de las funciones y actividades.
- El conocimiento se podrá acreditar en el certificado de funciones y/o a través de la evaluación directa durante la Fase III.

5. BAREMO APLICABLE A LA VALORACIÓN DE MÉRITOS

El baremo aplicable para la valoración de méritos se recoge en el Anexo I.

6. SISTEMA SELECTIVO EMPLEADO, PUNTUACIÓN DE LAS DIFERENTES FASES DEL PROCESO Y PUNTUACIONES MÍNIMAS PARA LA SUPERACIÓN DEL PROCESO

La evaluación de las candidaturas tendrá en cuenta su valoración en tres fases:

FASE I: Cumplimiento de requisitos imprescindibles.

Determinará la inclusión o exclusión en el proceso de selección.

FASE II: Valoración de méritos formativos y profesionales acreditados.

La puntuación máxima de esta fase será de 100 puntos y para superarla se deberá alcanzar un mínimo del 50% y su superación permitirá el acceso a la Fase III.

FASE III: Evaluación de competencias técnicas y competencias profesionales

La puntuación máxima para la evaluación de competencias técnicas será de 60 puntos, para la evaluación de competencias profesionales será de 40 puntos y para superarlas se deberá alcanzar un mínimo del 50% en cada una de ellas. Esta evaluación se realizará en base a pruebas y ejercicios selectivos específicos y entrevistas.

7. COMPOSICIÓN DEL ÓRGANO DE SELECCIÓN

El comité evaluador de este puesto estará compuesto por:

- El Director de Organización y Recursos Humanos.
- El Director de Tecnologías de la Información y la Comunicación.
- El Jefe del Departamento de Seguridad de la Información.

8. CONDICIONES ECONÓMICAS DEL PUESTO DE "ANALISTA PROGRAMADOR" DE SEGURIDAD DE LA INFORMACIÓN

Las retribuciones para esta posición son de 43.484,13 € brutos anuales fijos y hasta un máximo de un 10% de retribución variable, en función del cumplimiento de objetivos, evaluación competencial y disponibilidad presupuestaria.

9. PRESENTACIÓN DE CANDIDATURAS: FORMA Y PLAZOS

Quienes deseen participar en esta convocatoria deberán remitir su CV a la **dirección de correo electrónico** rrhh.empleo@selae.es, indicando en el **asunto** del correo lo siguiente: "AP Seguridad de la Información".

La **fecha límite** para la presentación de candidaturas será el día 15 de mayo de 2024, inclusive. No se evaluarán candidaturas remitidas con posterioridad a la fecha anteriormente señalada.

10. DURACIÓN MÁXIMA DEL PROCESO DE SELECCIÓN

Este proceso de selección se resolverá en un plazo máximo de seis meses.

Madrid, 24 de abril de 2024

La Sociedad Estatal Loterías y Apuestas del Estado, S.M.E., S.A. (en adelante SELAE), con domicilio social en C/ Poeta Joan Maragall, 53, 28020 Madrid, en cumplimiento de la normativa aplicable en materia de protección de datos personales, le informa, haciendo uso de la técnica por capas, que:

SELAE declara respetar escrupulosamente el derecho fundamental de las personas relativo al tratamiento de sus datos personales, y el estricto cumplimiento de lo dispuesto en la normativa de protección de datos:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos –RGPD–
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales –LOPDGDD-.–
- Así como la normativa de desarrollo que resulte de aplicación.

Epígrafe	*Información Básica*
Responsable	SOCIEDAD ESTATAL LOTERÍAS Y APUESTAS DEL ESTADO, S.M.E., S.A. (SELAE).
Finalidad	Los Datos Personales se tratarán para seleccionar a la candidatura más idónea, y su posterior contratación.
Legitimación	Interés legítimo por ambas partes de incluir a la persona candidata en un proceso de selección.
Destinatarios	No se publicarán ni cederán a terceros datos personales de las personas candidatas, salvo para el cumplimiento de las obligaciones legales aplicables en cada momento.
Derechos	Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Procedencia	Directamente de la propia persona candidata o bien a través de plataforma de selección que utilice.
Información Adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en: https://www.selae.es/f/loterias/web_corporativa/DatosPersonales/todos/vigente/Capa_II_Clausula_Seleccion_Personal.pdf

ANEXO I – BAREMO APLICABLE A LOS MÉRITOS VALORABLES

REQUISITOS PUBLICADOS EN EL PERFIL DEL PUESTO	CRITERIOS DE VALORACIÓN	PUNTUACIÓN Máximo 100 Puntos
3.1. REQUISITOS IMPRESCINDIBLES		
PUESTO	**TITULACIÓN**	
Analista Programador **Seguridad de la Información**	Titulación universitaria Nivel MECES 2 o superior, o sus equivalentes en títulos universitarios pre-Bolonia, en materia de Tecnologías de la Información y las Comunicaciones (TIC). Nivel B1 de idioma inglés.	No puntúa Requisitos excluyentes en el caso de no cumplimiento o no acreditación
	EXPERIENCIA	
Imprescindible un mínimo de 2 años de experiencia laboral demostrable en actividades de Seguridad de la Información, Seguridad TIC o Ciberseguridad.	Para la valoración de la experiencia será necesario el certificado acreditativo de la misma, donde conste la realización de las funciones y actividades objeto de la acreditación. Las candidaturas, tanto internas como externas, deberán aportar informe de vida laboral.	
MÉRITOS VALORABLES		
MÉRITOS ESPECÍFICOS (EXPERIENCIA) - Para la valoración de la experiencia será necesario el certificado acreditativo de la misma, donde conste la realización de las funciones y actividades objeto de la acreditación.		
Se valorará hasta un máximo de 4 años de experiencia como la anterior.	Se justificarán de la misma forma establecida para la acreditación de la experiencia requerida como imprescindible. Por cada 1 año completo adicional de experiencia, 12 puntos, hasta un máximo de 4 años adicionales (48 puntos).	Máximo 48 puntos
Se valorará la experiencia en: - Administración de sistemas (Linux RHEL, Windows, Active Directory). - Administración de equipos de comunicaciones y cortafuegos. - Administración de proxies de navegación web. - Criptografía aplicada (PKI, uso de OpenSSL, keytool, certutil, etc.). - Programación de scripts (al menos Python, sh y PowerShell). - SIEM. - Análisis de protocolos de comunicaciones (Wireshark o similares). - Elaboración de indicadores de Seguridad de la Información.	Se adjudicarán 8 puntos por cada uno de los apartados, hasta un máximo de 40 puntos.	Máximo 40 puntos
OTROS CONOCIMIENTOS ESPECÍFICOS		
Se valorará estar en posesión de una o más de las siguientes certificaciones profesionales en vigor: - ISC2 CISSP - ISACA CISM - ISO 27001 Auditor o Implementer - EC Council CEH - SANS GCIH - SANS GPEN - Offensive Security OSCP	Se adjudicarán 12 puntos por cada una de las certificaciones, hasta un máximo de 36 puntos.	Máximo 36 puntos
Se valorará el conocimiento de alguna de las siguientes materias: - Gestión de proyectos - SCRUM - Sistemas de Gestión de Seguridad de la Información - Esquema Nacional de Seguridad - Seguridad en Microsoft Exchange - Seguridad en Office365 - Seguridad en plataformas móviles (Android, iOS).	Se adjudicarán 12 puntos por el conocimiento de alguna de estas materias, hasta un máximo de 48 puntos.	Máximo 48 puntos
TITULACIÓN Y FORMACIÓN - Se justificarán mediante documentos o certificados acreditativos.		
- Los cursos deberán estar acreditados mediante títulos o diplomas y cuando varios de ellos se refieran a una misma materia, programa, aplicación, utilidad, etc, serán valorados como uno sólo: el de mayor nivel. **- Cuando en el título o diploma no conste el nivel del curso, éste será considerado como de nivel básico y se aplicarán las reglas de puntuación correspondientes a dicho nivel básico.**		
Se valorará estar en posesión de un título oficial y homologado de Máster y/o cursos de Postgrado en Ciberseguridad o Seguridad de la Información.	Se adjudicarán 24 puntos por la posesión de un Máster y 12 puntos por cada curso de Postgrado, hasta un máximo de 36 puntos.	Máximo 36 Puntos