Anexo de convocatoria

Técnico/a de Ciberseguridad Servicios Proactivos (INCIBE-CERT)

Subdirección INCIBE-CERT

ÍNDICE

1. DATOS DEL PUESTO 3
2. REQUISITOS MINIMOS PARA ACCEDER AL PROCESO DE SELECCIÓN .. 5
3. MÉRITOS A VALORAR 6
4. PRESENTACIÓN DE SOLICITUDES 7
5. FASES DEL PROCESO DE SELECCIÓN 8

5.1 Fase 1: valoración de méritos 8
5.2 Fase 2: conocimientos técnicos y entrevista 9

6. RESOLUCION DEL PROCESO 10

1. DATOS DEL PUESTO

- Puesto: Técnico/a de Ciberseguridad Servicios Proactivos (INCIBE-CERT)
- Número de efectivos: 1
- Grupo profesional: Técnicos
- Jornada: Completa
- Tipo de contrato: Indefinido (con 6 meses de período de prueba)
- Departamento/Proyecto: Subdirección Servicios INCIBE-CERT/Servicios Proactivos
- Localidad: León
- Retribución: Salario fijo de 24.636,27€ brutos anuales (variable en función de cumplimiento de objetivos y beneficios sociales)

- **Funciones del puesto:**

  - Participar en el desarrollo, operación y gestión de actividades y servicios de ámbito técnico como los siguientes:
    - Generación e intercambio de información e inteligencia sobre ciberamenazas y operación de herramientas para tal fin.
    - Ejercicios de entrenamiento y capacitación en ciberseguridad o ciberejercicios: jeopardys, red team – blue team, retos de ciberseguridad, roleplays, ingeniería social, simulación de ciberataques, todo ello a nivel nacional o internacional.
    - Vigilancia digital para detección, monitorización y análisis de eventos, amenazas e incidentes de ciberseguridad en fuentes abiertas, deep y dark web. Análisis y explotación de otra información, eventos e inteligencia en general en ciberseguridad disponible en INCIBE de otras fuentes o de herramientas propias.
    - Recolección de información de estado y evaluación sobre ciberseguridad, eventos de ciberseguridad y detección proactiva de incidentes de ciberseguridad, así como la realización de informes de exposición digital.
    - Investigación de amenazas, en los análisis detallados de aplicaciones maliciosas e investigaciones en relación con incidentes de ciberseguridad y su documentación.
    - Evaluación, diseño, desarrollo y operación de herramientas técnicas y utilidades para detección, monitorización y alerta temprana en ciberseguridad y de soporte a los servicios indicados o de nueva creación.
  - Participar en otras actividades de soporte y apoyo a la gestión de INCIBE-CERT como las siguientes:
    - Recopilación y análisis de indicadores de actividad de los servicios y colaboración en la elaboración de los reportes para seguimiento de la actividad de los servicios de INCIBE y el CERT.
    - Mantenimiento de información técnica operativa y de contacto de las entidades con las que colabora INCIBE-CERT.

- Contribuir a la mejora continua de los procesos del CERT, participando en el diseño, desarrollo y mantenimiento los procedimientos, herramientas, y técnicas documentadas, e incluyendo la integración con terceras partes implicadas.
- Comunicación de una forma efectiva con los públicos objetivos del CERT y con otros actores relacionados con la actividad del CERT (otros CERT, FCSE, ISP, etc.).
- Colaborar y asesorar a otros departamentos, representando los intereses y objetivos del CERT en proyectos y servicios controlados por otras áreas de la organización.
- Colaborar en la gestión de proyectos con proveedores externos, así como valorar la calidad del servicio ofrecido por estos. Llevar a cabo la elaboración de las condiciones de los contratos con proveedores que sean asignados en cada caso.
- Participar en intervenciones, eventos y foros de representación de INCIBE ante diferentes públicos, órganos e instituciones, correspondientes a su ámbito de actuación.

2. REQUISITOS MINIMOS PARA ACCEDER AL PROCESO DE SELECCIÓN

Los siguientes requisitos son excluyentes para avanzar en las siguientes fases del proceso de selección:

- Titulación académica de formación profesional de grado superior en Informática, o universitaria en Informática, Telecomunicaciones, Industriales, otras Ingenierías, CC Matemáticas, CC Físicas o análogas.
- Experiencia laboral de al menos 6 meses en alguna de las siguientes tareas de: Vigilancia digital de ciberamenazas; Capacitación y entrenamiento técnico en ciberseguridad; Generación y operación de inteligencia sobre ciberseguridad; Detección, monitorización e investigación y análisis de amenazas y malware. En todos los casos, en actividades similares a las descritas en las funciones del puesto.
- Nivel medio – B2- (hablado, lectura y escritura) de inglés.

3. MÉRITOS A VALORAR

Los méritos se baremarán siguiendo la distribución de puntuaciones que se indica en el apartado 5.1 del presente documento. El resultado de la suma de la puntuación en estos méritos será la que se tendrá en cuenta para avanzar en la fase 2 del proceso de selección.

Conocimientos, formación complementaria, otras titulaciones académicas, relacionados con las funciones del puesto y tareas a desempeñar, en particular:

- Formación:
  - Estar en posesión de un master, título de experto universitario y/o un doctorado relacionado con ciberseguridad.
  - Estar en posesión de certificaciones profesionales en Ciberseguridad (GIAC Certifications, ISC2 CISSP, Offensive Security OSCP, ISACA, CISA, ISACA, CISM, EC-Council CEH o ECIH) o similares
  - Formación específica sobre ciberseguridad en alguna de las siguientes materias:
    - Hacking ético / Pentesting y auditorías técnicas de ciberseguridad
    - Análisis de malware
    - Análisis forense
    - Ciberinteligencia
    - Vigilancia Digital
    - Ciberseguridad industrial
    - Ciberseguridad en dispositivos móviles.
  - Formación o certificación relacionada con redes u otra formación de interés para el puesto.
- Experiencia:
  - Experiencia demostrable adicional a la mínima en las actividades y servicios de ámbito técnico similares a las descritas en las funciones del puesto
  - Experiencia demostrable de trabajo en un CERT, en la gestión de proveedores externos, y/o de participación en eventos, foros o comunicaciones con ponencias, presentaciones o intervenciones.
  - Experiencia en el manejo de herramientas de ciberseguridad: herramientas de gestión de incidentes y herramientas específicas de Ciberseguridad tales como firewalls, IPS, IDS, SIEM, EDR/XDR, entre otras.
  - Otra experiencia y conocimientos en proyectos de investigación sobre ciberseguridad u otras actividades de ciberseguridad.
  - Experiencia en el uso de lenguajes de programación (Python, Perl, Bash, u otros de scripting) para su aplicación en el desarrollo de servicios de ciberseguridad.
- Nivel de idioma inglés superior al requerido.

4. PRESENTACIÓN DE SOLICITUDES

Los interesados que reúnan los requisitos del Anexo del puesto, deberán presentar su solicitud realizando los siguientes pasos:

- Paso 1: a través de la página Web de la Sociedad, cumplimentar el formulario correspondiente al puesto publicado en la sección de Empleo https://www.incibe.es/empleo
- Paso 2: realizado el anterior, recibirá un email indicando que para completar su inscripción es necesario el envío del currículum vitae al correo electrónico convocatorias@incibe.es indicando en el Asunto lo siguiente: **INC-DG02E-22007**

Obligatoriamente deberá incluirse un correo electrónico a través del cual se realizarán las comunicaciones relativas al proceso. La no presentación a cualquier prueba o entrevista a la que sean convocados supondrá la exclusión del proceso. Los candidato/as recibirán comunicación individual a través del correo electrónico facilitado del estado de su candidatura en el proceso de selección.

El plazo para la presentación de solicitudes será hasta el **20 de mayo de 2022, a las 14:00 horas.**

El envío del C.V. supone la declaración responsable de que todos los datos consignados son ciertos y comprobables a requerimiento de INCIBE, en cualquier fase del proceso y mediante cualquier documentación que se considere necesaria o útil en relación a los requisitos o méritos.

La valoración de méritos se realizará en función de los datos que se aporten en el CV así como la precisión de los mismos respecto a las fechas, funciones desarrolladas y conocimientos aportados por cada candidato/a.

5. FASES DEL PROCESO DE SELECCIÓN

La valoración de méritos se realizará en función de los datos que se aporten en el CV así como la **precisión** de los mismos respecto a las **fechas, funciones desarrolladas y conocimientos aportados** por cada candidato/a.

El proceso de selección para cubrir el puesto se realizará de acuerdo al procedimiento que a continuación se especifica:

5.1 Fase 1: valoración de méritos

De entre los candidatos que reúnan los requisitos de acceso, se llevará a cabo una valoración de los méritos relacionados con el desempeño del puesto (apartado 3 del presente anexo)

Esta valoración de méritos se efectuará con los siguientes criterios:

- Formación: En este apartado se valorarán los títulos académicos oficiales acreditados, los cursos de formación y especialización que sean relevantes en función del perfil del puesto y, en general, todos los elementos formativos que permitan estimar su adecuación.
  Puntuación máxima: 15

- Experiencia: Se valorará la experiencia profesional, en tanto sea semejante y/o de aplicación al perfil del puesto convocado.
  Puntuación máxima: 30

- Idiomas: En este apartado se valorarán nivel de idioma superior al requerido para el puesto, manejo de otros idiomas y/o estancias en el extranjero.
  Puntuación máxima: 5

La puntuación máxima en esta fase será de 50 puntos.

Pasarán a la siguiente fase del proceso aquellos candidatos que obtengan en esta fase al menos 20 puntos. Pasarán a la Fase II del proceso de selección un número de candidatos que pueda garantizar de manera suficiente la cobertura de vacantes en cada caso.

5.2 Fase 2: conocimientos técnicos y entrevista

Se evaluará el perfil profesional de los candidatos que pasen a esta fase a través de dos pruebas:

- Conocimientos técnicos: en este criterio la Comisión de selección decidirá la metodología más adecuada para la valoración de los conocimientos técnicos, pudiendo consistir en una prueba escrita o/y entrevista de conocimientos técnicos.
  Puntuación máxima: 20

- Entrevista competencial: esta entrevista personal tendrá como objeto estimar las mejores actitudes y aptitudes competenciales de gestión de los candidatos en relación con las funciones y tareas del puesto a desempeñar. Las competencias requeridas a valorar: Orientación al logro, Trabajo en equipo, Colaboración y Compromiso y Autoaprendizaje.
  Puntuación máxima: 20

La puntuación máxima en esta fase será de 40 puntos.

La puntuación mínima para superar la prueba de conocimiento y la entrevista personal será de 10 puntos. Ambas pruebas de conocimientos técnicos y entrevista competencial son excluyentes, resultando necesario superar ambas para superar la Fase II.

Las Fases I y II son excluyentes, resultando necesario superar ambas para ser un candidato/a apto/a en el proceso de selección.

6. RESOLUCION DEL PROCESO

INCIBE se reserva la posibilidad de cubrir el número de puestos que estime oportuno, declarando desierto el resto.

Se convocará a los aspirantes seleccionados para suscribir los correspondientes contratos de trabajo en la modalidad prevista en el Anexo.

Se creará una bolsa de trabajo con los candidatos que habiendo superado el proceso selectivo finalmente no hayan obtenido el puesto. Con esta lista se podrán cubrir vacantes del mismo perfil durante un período de un año.

Si algún candidato no presentase en el plazo señalado la documentación requerida para la celebración del contrato, o no superase el periodo de prueba establecido, INCIBE requerirá al siguiente candidato de la bolsa de trabajo.