INSTITUTO NACIONAL DE CIBERSEGURIDAD

ANEXO DE CONVOCATORIA

- **Puesto:** Técnico/a de Tecnologías Ciberseguridad
- **Número de efectivos:** 6
- **Grupo profesional:** Técnicos
- **Departamento/Proyecto**: Tecnologías/Operaciones
- **Tipo de contrato:** Indefinido
- **Jornada:** Completa
- **Localidad**: León
- **Bolsa de empleo:** Si
- **Reserva personas con discapacidad:** 3

FUNCIONES

- Administrar y desarrollar aspectos técnicos de la gestión de proyectos, utilizando adecuadamente las herramientas o soluciones necesarias.
- Investigar soluciones aplicables en el ejercicio de su función para aportar valor añadido y diferenciación a la actividad de INCIBE.
- Analizar y participar en el diseño de los requisitos de los proyectos en los que participa, de acuerdo a la metodología y procesos definidos en el área.
- Diseñar, desarrollar, modificar, adaptar e implementar soluciones según las necesidades de la organización y de sus clientes, así como revisar los requerimientos del sistema y validar y testear las soluciones a implantar en base a los estándares de calidad establecidos.
- Asesorar a otros departamentos de INCIBE y al cliente final (sobre soluciones planteadas, consultas e incidencias, etc.), en lo que respecta al desarrollo de proyectos de su ámbito de actuación.
- Colaborar en la gestión de proyectos con proveedores externos, así como valorar la calidad del servicio ofrecido por estos y compartir dichas valoraciones con sus responsables.
- Colaborar en la implantación u operación de los sistemas de gestión de INCIBE
- Colaborar en la elaboración de los reportes necesarios para el correcto seguimiento de la actividad de los proyectos a sus supervisores u otros departamentos de INCIBE.
- Participar en la elaboración de las condiciones técnicas de los contratos con proveedores.

La adscripción a las tareas descritas no supone ningún tipo de limitación en cuanto a movilidad funcional.

REQUISITOS PARA ACCEDER AL PROCESO DE SELECCIÓN

Titulación y Formación complementaria:

- Titulación universitaria en Informática, Telecomunicaciones, Ingenierías, CC Matemáticas, CC Físicas o titulación académica de formación profesional de grado superior en Informática, o análogas a las anteriores.

Experiencia Profesional:

- Experiencia laboral de 1 año relacionada con las funciones del puesto.

Idiomas:

- Nivel medio de inglés.

MÉRITOS A VALORAR

Conocimientos, formación complementaria, otras titulaciones académicas, experiencia profesional relacionados con las funciones del puesto y tareas a desempeñar, entre las que se pueden encontrar:

- Formación adicional, otras titulaciones y certificaciones profesionales tales como CISSP, CSSLP, CEH, ECSP, OSCP u otras de contenidos análogos.
- Publicaciones de investigación realizadas en el campo de la ciberseguridad, ponencias de alto valor técnico en eventos de ciberseguridad, participación en proyectos internacionales y menciones o premios recibidos en este ámbito.
- Nivel de inglés superior al mínimo requerido.
- Gestión de proyectos: metodologías de gestión, definición, planificación, seguimiento y control, gestión de proveedores externos, ejecución de proyectos y herramientas de gestión.
- Ciberseguridad: integración, investigación y análisis de eventos de ciberseguridad para la detección proactiva de incidentes, tendencias e indicadores, *botnets*, *sink-holing*, técnicas *hacking*, sistemas trampa o señuelos, ingeniería y análisis de *malware*, análisis de vulnerabilidades, *exploits*, gestión de incidentes, análisis forense, métodos de investigación de la cibercriminalidad, de logs y de evidencias.
- Herramientas tecnológicas: conocimientos específicos de SIEM, IDS, *honeypots*, análisis de malware, y otras herramientas orientadas a la ciberseguridad.
- Experiencia y formación específica en *pentesting*, y/o en auditorías de seguridad de aplicaciones.
- Operación y mejora de herramientas de ciberseguridad.
- Competencias: planificación y organización, orientación al logro, autoaprendizaje, innovación y creatividad, orientación al cliente, pensamiento analítico, adaptabilidad y flexibilidad, trabajo en equipo.

Adicionalmente se valorarán los conocimientos y experiencia profesional en al menos una de las siguientes áreas:

- ***Inteligencia en ciberseguridad****:*
  - *Threat intelligence*.
  - Uso de tecnologías *BigData* y *Business Intelligence & Analytics.*
  - Ciberinteligencia: OSINT, correlación de eventos, IDS/IPS, análisis de logs, scripting, amenazas y vulnerabilidades emergentes, análisis de malware, DFIR, estándares de intercambio de información, modelos *Kill Chain* y/o Diamante, así como experiencia en el uso de herramientas relacionadas.
- ***Sistemas de control industrial:***
  - Despliegue, operación y soporte de tecnologías de ciberseguridad industrial.
  - Análisis de vulnerabilidades, honeypots, análisis de malware, etc, orientados a SCI.
  - Seguridad de sistemas, procesos y protocolos de control industrial: analizadores de vulnerabilidades orientados a sistemas de supervisión y control, herramientas avanzadas basadas en técnicas de análisis inteligentes de datos para la supervisión de procesos industriales, redes trampa orientadas a sistemas de supervisión y control, diseño e implantación de sistemas de supervisión y control de procesos industriales, formación especializada en sistemas de automatización industrial y/o ciberseguridad, sistema de detección de intrusos (IDS) y monitorización de red, programación de sistemas de control industrial y colaboración demostrable en distribuciones Linux orientadas a ciberseguridad industrial.
- ***Desarrollo de tecnologías de ciberseguridad:***
  - Tecnologías orientadas al desarrollo de software: lenguajes de programación; tecnologías, servicios y servidores web; ansible o similares; tecnologías ELK o similares; sistemas operativos; BBDD; gestión de colas de trabajo o de trabajos distribuidos; herramientas de testing y de integración continua.
  - Metodologías de desarrollo de software: metodologías, marcos de trabajo o buenas prácticas en desarrollo y mantenimiento de software; desarrollo tradicional y ágil; evaluación de calidad de producto software.
  - Seguridad y desarrollo seguro del software: arquitectura y modelos de seguridad, sistemas y metodología de control de acceso, seguridad de las operaciones, criptografía, seguridad física, seguridad en internet, redes y telecomunicaciones, recuperación ante desastres y planificación de la continuidad del negocio. Desarrollo seguro de aplicaciones software.
  - Proyectos en que se haya participado de desarrollo y mantenimiento software, especialmente los relacionados con análisis forense, visión artificial, tratamiento de datos, aprendizaje automático, calidad del software, y ciberseguridad o su investigación.
- ***Análisis en ciberseguridad:***
  - Ciberseguridad en general y en las siguientes áreas en particular: ingeniería y análisis de malware, técnicas hacking, señuelos, análisis de vulnerabilidades y *exploits*, análisis forense y métodos de investigación de logs y de evidencias.
  - Conocimientos e investigaciones realizadas sobre el cibercrimen.
  - Alta creatividad orientada a la investigación en ciberseguridad.

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 el siguiente: INC-DO02A-18010.

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.

El plazo para la presentación de solicitudes será hasta el **5 de noviembre de 2018 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

Aquellos aspirantes con grado de discapacidad igual o superior al 33% que deseen participar en el proceso selectivo deberán advertirlo al enviar la solicitud, indicando las adaptaciones de medios y/o tiempo necesarias para la realización de las pruebas.

Fase I

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. Pasarán a la siguiente fase del proceso aquellos candidatos cuyos méritos mejor se ajusten al perfil deseado.

Fase II

Para evaluar que el perfil profesional del candidato se ajusta al puesto la valoración se basará en la información y documentación aportada por los aspirantes, que será completada con las pruebas y/o entrevistas técnicas y personales que en cada caso se determinen.

Resolución del proceso

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

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, ordenada por los resultados del proceso. 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.