RESPONSABLE ÁREA DE SEGURIDAD

Misión:

Con carácter general se encargará de definir e implantar la política de seguridad de la información, normativas, procedimientos estándares y directrices asociados a la seguridad de la información para garantizar el cumplimiento legal. Definir las medidas de seguridad, física y lógica a aplicar y coordinar su implantación, así como gestionar los contratos del área.

Características del puesto:

Tipo de Contrato: temporal

Lugar de Trabajo: Zaragoza

Salario: (A1: Licenciado, Ingeniería Superior, Grado) N26B: 41.668,50 €
(A2: Diplomado, Ingeniero Técnico, Grado) N26B: 39.280,52 €

Funciones del Puesto:

Creación, mantenimiento y custodia de la normativa sobre seguridad de la información de la entidad

Gestionar y custodiar las herramientas necesarias de ciberseguridad así como los elementos de las que se compongan

Establecer las políticas y necesidades al respecto del respaldo de información

Establecer y mantener la normativa técnica a aplicar en materia de seguridad

Cumplir y hacer cumplir las normas y procedimientos en materia de seguridad integral, establecidos por AST

Marcar las directrices técnicas necesarias para asegurar la identidad digital de la entidad

Gestión, control y supervisión de los requisitos de seguridad de la información y de los servicios, acorde al ENS y RGPD.

Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en el ámbito del cumplimiento del ENS.

Recolectar información sobre los activos a securizar

Determinar los niveles de seguridad de la información en relación a la aplicación del Esquema Nacional de Seguridad y del RGPD.

Orientar y formar a los usuarios para la concienciación y el uso seguro de las TIC

Participar y liderar reuniones de trabajo relacionadas con el área

Elaborar, ejecutar y coordinar el plan de trabajo conjuntamente con el superior inmediato

Elaborar informes periódicos de las actividades realizadas y reportar al superior

Generar toda la documentación asociada a los trabajos realizados

Trabajar de manera transversal con otras áreas y direcciones de la entidad, de los departamentos del Gobierno de Aragón y de otras entidades públicas

Participar y colaborar en aquellos foros en materia de seguridad en los que colabore AST

Trabajo conjunto en la medida de los requerimientos con las Fuerzas y Cuerpos de Seguridad del Estado.

Atender los requerimientos del Poder Judicial en torno a las solicitudes que realice a AST o en esta deleguen otros entes del Gobierno de Aragón

Instar y asesorar en la valoración de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información por parte de los nuevos servicios electrónicos

Creación y mantenimiento de cláusulas de confidencialidad en los contratos con terceras partes y velar por su inclusión y por su cumplimiento.

Realizar o instar a la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad TIC

Monitorizar el estado de la seguridad de los sistemas proporcionado por las herramientas de gestión de eventos de seguridad u otros mecanismos de auditoría implementados

Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución

Analizar los riesgos del ecosistema TIC y proponer mejoras.

Establecer y mantener los planes de mejora continua en el marco de la continuidad de negocio y la Seguridad TIC.

Requisitos mínimos exigidos:

-Tener acreditada una experiencia laboral de al menos 2 años en puestos de similares características (Responsable de Seguridad. Análisis de Riesgos de seguridad TIC. Implementación de ENS – ISO 27001 o análogas, o trabajos análogos a las funciones descritas)

-Licenciado, Ingeniero Superior, Grado (Nivel A1) o Diplomado, Ingeniero Técnico o Grado (nivel A2)

-Formación mínima de 20 horas en Seguridad de la Información (ENS-ISO27001 o análogas)

Criterios de Selección

1.Fase de Concurso:

1.1. Se valorará en esta fase con un máximo de 10 puntos la formación en temas de seguridad, gestión de proyectos TI, formación en ITIL, LOPD-RGPD, ENS-ISO27001, seguridad informática, productos de seguridad y respuestas a incidentes de seguridad, Esquema ENI y Auditoría técnica (backing). (5 puntos por máster, 2 puntos certificaciones, 1 punto formación más de 25 horas y 0,5 puntos formación menos de 25 horas) (Se acreditarán mediante certificación académica)

1.2. Experiencia profesional con un máximo de 30 puntos en: Implantación de ENS ISO 27001 o análogas (2,5 puntos por año completo con un máximo 10 puntos), Análisis de Riesgos TIC y auditorías de seguridad (2,5 puntos por año completo con un máximo 5 puntos), experiencia en trabajos con los esquemas ENI/ENS (2,5 puntos por cada año completo como máximo 5 puntos), Auditor y trabajos relacionados con la seguridad informática en general (2,5 puntos por cada año completo con un máximo 5 puntos). (Se acreditará mediante CV+ vida laboral+ Certificado de empresa o Contrato)

Experiencia como trabajador para Administraciones Públicas en el ámbito relacionado al puesto (1 punto por año trabajado con un máximo de 5 puntos)

2. Fase de valoración de conocimientos

2.1. Ejercicio 1. Puntuación máxima 12 puntos y corresponderá a un cuestionario de test relacionado con el temario detallado (incluido como Anexo). Esta prueba se calificará de 0 a 12 puntos. La nota mínima para mediar es de 3,6 puntos.

2.2 Ejercicio 2. Puntuación máxima 12 puntos. Desarrollo y resolución de un supuesto práctico sobre el temario detallado. Esta prueba se calificará de 0 a 12 puntos. La nota mínima para mediar es de 3,6 puntos.

2.3. Ejercicio 3. Puntuación máxima 6 puntos. Cuestionario psicotécnico de razonamiento lógico. Esta prueba se calificará de 0 a 6 puntos mediante puntuación centil de rango 0-99. La nota mínima para mediar es de 1,8 puntos

Sólo pasarán a la siguiente fase los que alcancen una puntuación mayor o igual a 15 puntos en la suma de los 3 ejercicios. No obstante, la Comisión de selección podrá adaptar la puntuación mínima posible prevista.

La Comisión de Selección podrá considerar que los candidatos que no consigan la plaza entren en una bolsa de empleo si obtienen una puntuación mayor o igual a 6 puntos en cualquiera de los dos ejercicios 1 y 2.

3. Fase de entrevista

Los candidatos que hayan superado las notas de corte en las anteriores fases serán convocados a la fase de entrevista.

3.1. Entrevista con el INAEM que, además de ratificar los conocimientos y experiencia, se valorarán las competencias asociadas al puesto y detalladas en la descripción del mismo. Tendrá una puntuación máxima de **20 puntos** en función de la mayor adecuación al perfil solicitado.

3.2. Entrevista con la Comisión de Selección que valorará los aspectos más significativos para la idoneidad del puesto como motivación, predisposición, trabajo en equipo, etc. Tendrá una puntuación máxima de **10 puntos.**

Los candidatos interesados en participar del proceso de selección deberán llamar al ESPACIO EMPRESAS DEL INAEM DE ZARAGOZA teléfono 976716219 de 9:00 a 14:00 horas indicando el número de oferta de empleo 02-2018-007672. Deberán acreditarse adjuntando el CV los méritos que deseen aportar. El plazo de presentación de la candidatura finaliza el día 1 de agosto de 2018.

ANEXO

Temario

Planificación y control de las TIC: Gestión de servicios e infraestructuras TIC, gestión del valor de las TIC. Acuerdos de Nivel de Servicio. Gestión de incidencias. Bases conceptuales de ITIL (IT Infrastructure Library), y CoBIT (Control Objetives for Information and Related Technology), objetivos de control y métricas

El cumplimiento normativo. GDPR. Politicas de Seguridad.. El Esquema Nacional de Seguridad. Adecuación al Esquema Nacional de Seguridad. Estrategia Nacional de Seguridad. CCN-STIC.. Instituciones de interés AEPD, CCN, FFCCS, CERT's, etc.

Delitos informáticos y legislación. Investigaciones forenses digitales.

Análisis y gestión de riesgos. Herramientas. Auditorias relacionadas con seguridad

Planes de recuperación de desastres (DR) y continuidad del negocio. Políticas de Backup. Planes de pruebas

Concienciación y formación en materia de seguridad.

Implantación de Sistemas de Gestión de la Seguridad en la Información (SGSIS).

Interoperabilidad de sistemas (1). El Esquema Nacional de Interoperabilidad. Dimensiones de la interoperabilidad.

Interoperabilidad de sistemas (2). Las Normas Técnicas de Interoperabilidad. Interoperabilidad de los documentos y expedientes electrónicos y normas para el intercambio de datos entre Administraciones Públicas.

Dominio 1: Conceptos de ciberseguridad. Riesgo, tipos y vectores de ataque, políticas, procedimientos y controles

Dominio 2: Principios de arquitectura de seguridad. El modelo OSI, defensa en profundidad, cortafuegos, segmentación, monitorización, detección, registro y encriptación.

Dominio 3: Seguridad de redes, sistemas, aplicaciones y datos. Evaluación del riesgo, gestión de vulnerabilidades, test de penetración, seguridad de la red, SO, aplicaciones y datos.

Dominio 4: Respuesta ante incidentes. Respuesta ante incidentes de seguridad, investigación, retención legal, preservación, estudios forenses, DRP y BCP.

Dominio 5: Implicaciones de seguridad y adopción de tecnologías en evolución. Amenazas actuales, APTs, tecnologías móviles, consumerización de las TI, cloud y colaboración digital. Implantación de herramientas para gestión y monitorización de eventos de seguridad (SIEM).