Convocatoria interna y externa

La Secretaría de Integración Económica Centroamericana invita a participar en la convocatoria de la siguiente posición con sede en la ciudad de Guatemala, para una plaza indefinida **100%** presencial **(no remota)**

Administrador(a): Seguridad Informática "Senior"

Objetivo del puesto:
Gestionar iniciativas de seguridad informática reflejadas en normativas, medidas y controles, verificando el cumplimiento del Manual de sistema de gestión de la seguridad de la información de la SIECA.

Formación académica:
Graduado de Ingeniería en Sistemas, Licenciatura en Informática, carrera afín, en caso de no tener título universitario, demostrar experiencia de 10 años en el área.

Especialización en Seguridad Informática, con alguna de las siguientes certificaciones de seguridad de la información como CISSP, CISM, CISA, ISO 27001 lead implementer, CSSP.

Otros cursos y seminarios:

- *Análisis Forense*
- *Ethical Hacking*
- *Protocolos de seguridad (IPSec)*
- *Análisis de vulnerabilidades*
- *Trabajo en equipo*
- *Relaciones humanas*
- *Administración del tiempo*

Funciones del puesto:

1. Cumplir con las políticas, lineamientos y disposiciones establecidos en los diferentes manuales administrativos y normativas de la Secretaría de Integración Económica Centroamericana (SIECA) y los correspondientes a los Proyectos de Cooperación cuando aplique, según el convenio de cooperación.
2. Experiencia en la identificación, evaluación y gestión de riesgos de seguridad de la información.
3. Habilidad para realizar evaluaciones de vulnerabilidades y análisis de amenazas.
4. Capacidad para desarrollar, implementar y mantener políticas de seguridad y procedimientos que cumplan con las normativas y estándares de la industria.
5. Conocimiento de arquitecturas de red y sistemas, así como experiencia en la implementación de controles de seguridad a nivel de red y aplicación.

6. Conocimientos avanzados en prácticas de seguridad en el desarrollo de software, integrando medidas de seguridad desde las fases iniciales del ciclo de vida del desarrollo (DevOps, DevSecOps).
7. Experiencia en liderar equipos de respuesta a incidentes, así como la capacidad para coordinar la identificación, mitigación y recuperación de incidentes de seguridad.
8. Conocimientos en técnicas de análisis forense digital y capacidad para dirigir investigaciones en casos de ataques de seguridad.
9. Experiencia en asegurar que la organización cumpla con las regulaciones y normativas de seguridad relevantes en su industria (ISO 27001).
10. Habilidad para desarrollar programas de concientización y formación en seguridad para el personal de la SIECA.
11. Conocimientos en seguridad en la nube AWS, incluyendo la configuración segura de servicios en AWS y la gestión de la seguridad de los datos en entornos de nube.
12. Dar seguimiento, en coordinación con la dirección o unidad responsable de la administración del Sistema de Gestión de Seguridad de la Información para solucionar las No conformidades internas y externas resultado de auditorías, así como a la identificación de oportunidades de mejora.
13. Realizar cualquier otra labor que le sea asignada por el/la jefe(a) inmediato(a).

Experiencia laboral:
Cinco años en puestos similares, gestionando políticas y procedimientos de seguridad informática y participando en procesos de auditoría de seguridad de información.

Habilidades básicas, técnicas, otras:

Deseable:
- Experiencia laboral en organizaciones similares.
- Conocimiento de administración de equipos de seguridad perimetral: firewall, antispam, domain controller, entre otros.
- Con experiencia en procesos de certificación ISO 20000-1 y 27001.

Competencias técnicas:
De conocimiento
- Normativa ISO 20000-1 y 27001
- Entender leyes y normativas, estar actualizado en herramientas de seguridad y desarrollar habilidades en la gestión de incidentes de seguridad de la información.

De dominio
- Conocimientos avanzados de seguridad, tecnologías de red y nube AWS, sistemas operativos Windows y Linux, criptografía, gestión de identidad, seguridad de aplicaciones y protocolos.

NOTA:

1. Únicamente serán tomadas en cuenta las aplicaciones remitidas a la casilla electrónica talentoycultura@sieca.int con copia a msoto@sieca.int y que tengan **adjunto el formato Cv-SIECA en PDF editable, su Cv y constancias que acreditan el grado académico y cursos recibidos.**

2. El plazo de la convocatoria vence el **3 de mayo de 2024** a las 11:59 p.m.

La SIECA está comprometida con la consecución de la diversidad en su fuerza laboral, y motiva a todas las personas calificadas a postularse, independientemente de su género, nacionalidad, capacidades, orientación sexual, así como de sus antecedentes culturales, religiosos y étnicos.

La SIECA, como órgano técnico administrativo del Proceso de Integración Económica Centroamericana, promueve y favorece el desarrollo y contratación de nacionales de los países miembros del Subsistema de Integración Económica Centroamericana (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá).

Para ello la contratación de nacionales del Subsistema de Integración Económica Centroamericana se atenderá a la capacidad, idoneidad y disponibilidad en igualdad de condiciones para todos los países miembros, conforme las posibilidades y necesidades de la SIECA.

En casos debidamente calificados o justificados, podrán participar personas de otras nacionalidades en los procesos de contratación de la SIECA.

Lineamientos para aplicar:

1. Leer todos los requisitos solicitados en esta convocatoria, adjuntando: Curriculum vitae, constancias que acrediten grado académico y constancias de capacitaciones recibidas.

2. Descargar y guardar en su computadora personal el archivo en PDF editable denominado **Formato CV SIECA-editable.** Completar todos los datos requeridos y guardar el archivo nuevamente con: apellido y nombre del postulante y nombre del puesto.

3. Asegurarse de incluir en el correo electrónico:

a. Archivo de Cv-SIECA **lleno y grabado con las especificaciones requeridas en el numeral 2**.
b. Curriculum vitae y constancias que acrediten el grado académico obtenido y capacitaciones recibidas.

FAVOR ADJUNTAR A LA APLICACIÓN
QUE ENVIARÁ (EN EL CUERPO DEL CORREO ELECTRÓNICO),
ESTE CUADRO CON LAS RESPUESTAS A SU NIVEL DE DOMINIO.

NRO.	¿Posee experiencia en…?	SI/NO	Puesto en el que ejecutó tal experiencia	Tiempo de experiencia en años	Institución
1	¿Su aspiración salarial es negociable? En caso de sí serlo, por favor en el cuadro de la par, indique el monto negociable en dólares.				
2	Esta posición es de carácter indefinido “planilla”, la modalidad de labores del puesto es 100% presencial (no híbrida, no remota) en la ciudad de Guatemala. Si fuera seleccionado(a) para ocupar la vacante, deberá trasladarse a vivir a Guatemala. ¿Estaría de acuerdo con la metodología y el traslado de país?				
3	¿Tiene experiencia en la identificación, evaluación y gestión de riesgos de seguridad de la información?				
4	¿Ha realizado evaluaciones de vulnerabilidades y análisis de amenazas?				
5	¿Ha desarrollado, implementado y brindado mantenimiento a políticas de seguridad y procedimientos que cumplan con las normativas y estándares de la industria?.				
6	¿Tiene conocimiento de arquitecturas de red y sistemas, así como experiencia en la implementación de controles de seguridad a nivel de red y aplicación?				
7	¿Tiene experiencia en liderar equipos de respuesta a incidentes, así como la capacidad para coordinar la identificación, mitigación y recuperación de incidentes de seguridad?				

8	¿Tiene experiencia en asegurar que la organización cumpla con las regulaciones y normativas de seguridad relevantes en su industria (ISO 27001)?				
9	¿Ha desarrollado programas de concientización y formación en seguridad para el personal de la empresa para la que ha laborado?				
10	¿Ha brindado seguimiento al sistema de Gestión de Seguridad de la Información para solucionar las No conformidades internas y externas resultado de auditorías?				
11	¿Ha gestionado políticas y procedimientos de seguridad informática y participando en procesos de auditoría de seguridad de información?				
12	¿Experiencia laboral en organizaciones similares a la SIECA?				
13	¿Tiene conocimiento de administración de equipos de seguridad perimetral: firewall, antispam, domain controller, entre otros?				
14	¿Cuenta con experiencia en procesos de certificación ISO 20000-1 y 27001?				
15	¿Es graduado de Ingeniería en Sistemas, Licenciatura en Informática, carrera afín, en caso de no tener título universitario tiene experiencia comprobable de 10 años en el área?				
16	¿Tiene especialización en Seguridad Informática, con alguna de las siguientes certificaciones de seguridad de la información como CISSP, CISM, CISA, ISO 27001 lead implementer, CSSP?				
17	¿Tiene cinco años de experiencia en puestos similares, gestionando				

	políticas y procedimientos de seguridad informática y participando en procesos de auditoría de seguridad de información?				

NRO.	Preguntas sobre habilidades, técnicas, etc. Favor especificar	SI/NO	Nivel de conocimiento adquirido (no lo tiene/básico/intermedio/ avanzado)
1	¿Tiene conocimientos en prácticas de seguridad en el desarrollo de software, integrando medidas de seguridad desde las fases iniciales del ciclo de vida del desarrollo (DevOps, DevSecOps)?		
2	¿Qué nivel de conocimientos tiene en técnicas de análisis forense digital y capacidad para dirigir investigaciones en casos de ataques de seguridad?		
3	¿Qué nivel de conocimientos tiene en seguridad en la nube AWS, incluyendo la configuración segura de servicios en AWS y la gestión de la seguridad de los datos en entornos de nube?		
4	¿Conoce de la normativa ISO 20000-1 y 27001?		
5	¿Ha actualizado herramientas de seguridad y desarrollado habilidades en la gestión de incidentes de seguridad de la información?		
5	¿Tiene conocimientos de seguridad, tecnologías de red y nube AWS, sistemas operativos Windows y Linux, criptografía, gestión de identidad, seguridad de aplicaciones y protocolos?		