CONVOCATORIA - DEPARTAMENTO DE TALENTO Y CULTURA - SIECA

La Secretaría de Integración Económica Centroamericana (SIECA) con sede en la ciudad de Guatemala, le invita a participar en la presente convocatoria para optar a la siguiente vacante laboral (contratación por plazo indefinido y 100% presencial en la sede de la SIECA/no remota):

Administrador(a) "B": Seguridad Informática

Con enfoque en procesos y políticas de seguridad de la información

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:
Estudiante del último año de las carreras de Ingeniería en Sistemas, Licenciatura en Informática, carrera afín o 5 años de experiencia en el área; con especialización en Seguridad Informática.

Otros cursos y seminarios:

- Análisis Forense, ISO 27001, Ethical Hacking, Análisis de vulnerabilidades, Protocolos de seguridad (IPSec). Capacitaciones sobre trabajo en equipo, relaciones humanas, administración del tiempo, manejo de estrés laboral.

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. Identificar y evaluar riesgos de seguridad, y desarrollar estrategias para mitigarlos.
3. Mantenerse actualizado de las últimas amenazas y tecnologías de seguridad de al menos los últimos 3 meses, implementando actualizaciones y mejoras según sea necesario.
4. Trabajar en estrecha colaboración con otras direcciones de la SIECA, para garantizar la integración de la seguridad en todas las áreas de la organización.
5. Acompañar junto con la dirección o unidad responsable de las auditorías externas e internas del sistema de gestión de seguridad de la información.
6. Crear y mantener políticas y procedimientos de seguridad de la información alineados a la normativa ISO/IEC 27001:2022.
7. Implementar y dar seguimiento al cumplimiento de controles y proyectos de ciberseguridad.
8. Coordinar y responder a incidentes de seguridad, investigar incidentes y asegurar que las medidas correctivas sean eficaces.

9. Impartir programas de concientización sobre seguridad y proporcionar capacitación regular para el personal de la empresa.
10. Planificar, ejecutar y evaluar campañas internas de pruebas de phishing, analizando los resultados y ajustando los programas de concientización y capacitación según los hallazgos obtenidos.
11. Liderar la identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información, manteniendo actualizadas las matrices de riesgos, activos, amenazas, controles y planes de tratamiento, en cumplimiento con el ciclo de vida del SGSI.
12. Desarrollar, implementar y mantener la matriz de clasificación de la información, asegurando que todos los activos de información estén clasificados de acuerdo con su nivel de sensibilidad y estableciendo medidas de seguridad adecuadas para cada categoría.
13. Realizar auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad y los estándares establecidos.
14. Dar seguimiento, en coordinación con la dirección o unidad responsable del Sistema de Gestión de Seguridad de la Información, para solucionar las No conformidades internas y externas resultado de auditorías, así como identificar oportunidades de mejora.
15. Asegurar la implementación adecuada de controles de seguridad física y lógica para proteger los activos de información.
16. Asegurar la continuidad del negocio mediante la implementación, mantenimiento y ejercicios del plan de recuperación ante desastres (DRP), plan de continuidad de negocios (BCP) y plan de recuperación del negocio (BRP) y respaldo de datos.
17. Dar seguimiento y análisis a los KPI de ciberseguridad para evaluar el desempeño y efectividad de las actividades y controles implementados.
18. Realizar cualquier otra labor relacionada a Ciberseguridad que le sea asignada por el/la jefe(a) inmediato(a), con la capacidad de asumir temporalmente funciones adicionales en caso de ausencias, garantizando la operatividad del área.

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

Requisitos deseables:
1. Experiencia en la implementación y gestión de sistemas de gestión de seguridad de la información (SGSI) bajo normativas: ISO/IEC 27001.
2. Conocimientos y experiencia práctica en la gestión de riesgos de seguridad de la información y auditorías internas.
3. Experiencia en la planificación y ejecución de planes de continuidad de negocio y recuperación ante desastres.

4. Conocimiento avanzado en políticas de seguridad, controles de seguridad física y lógica, y gestión de riesgos.
5. Capacidad para diseñar e implementar programas de concientización y capacitación en seguridad informática.
6. Experiencia en la implementación de controles de ciberseguridad, como protección de datos y medidas de protección perimetral.

Habilidades básicas, técnicas, otras:

- Nivel intermedio de idioma extranjero/inglés
- Manejo avanzado de paquete de programas informáticos de Microsoft Office y otras herramientas de gestión virtual

Competencias de Conocimiento

- Normativa ISO/IEC 20000-1 e ISO/IEC27001
- Entender leyes y normativas, estar actualizado en herramientas de seguridad y desarrollar habilidades en la gestión de incidentes.

Competencias de dominio

- Fundamentos de seguridad, tecnologías de red, sistemas operativos, criptografía, gestión de identidad, seguridad de aplicaciones y protocolos.
- Visión estratégica, toma de decisiones, comunicación efectiva, empoderamiento de equipos, capacidad de influencia, pensamiento crítico y resolución de problemas, gestión del cambio, fomento de la colaboración, resiliencia

INFORMACIÓN IMPORTANTE:

Lineamientos para aplicar:

1. Leer detenidamente la convocatoria y seguir enteramente las instrucciones que allí se indican.

2. Descargar, completar e incorporar los formatos adjuntos en la convocatoria como parte de su postulación.

3. Remitir su postulación a la casilla electrónica reclutamientos@sieca.int con copia al correo msoto@sieca.int incorporando en adjunto como mínimo lo siguiente:
   - Formato CV_SIECA en PDF editable completado (descargar el archivo del sitio web de la SIECA)
   - Cuadro con información complementaria completado (descargar el archivo del sitio web de la SIECA)

- Hoja de vida actualizada.
- Título universitario de grado y/o pregrado, cierre de pénsum universitario, certificado de notas del grado universitario obtenido, título a nivel diversificado (según aplique con base a lo requerido para la vacante).
- Constancias que acrediten cursos recibidos (según aplique con base a lo requerido para la vacante).

4. Su postulación debe remitirse a más tardar el **11 de agosto del año 2025** a las 23:59 horas, ya que, posterior a ello no se tomará en cuenta.

Observaciones:

- 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.