



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 (no híbrida ni remota) en la sede de la SIECA-

Administrador: Seguridad Informática

Objetivo del puesto:

Gestionar, implementar y fortalecer la seguridad de la información y la ciberseguridad institucional de la SIECA, mediante la identificación, evaluación y mitigación de riesgos; la administración de controles, accesos, herramientas de monitoreo y protección tecnológica, la respuesta oportuna a incidentes y la mejora continua de los mecanismos de prevención, detección y remediación, asegurando la protección, confidencialidad, integridad, disponibilidad y resiliencia de la infraestructura tecnológica, los sistemas y los datos institucionales, en cumplimiento de las políticas, normativas internas y disposiciones aplicables.

Formación académica:

Estudiante de las carreras de Ingeniería en Sistemas, Licenciatura en Informática, carrera afín o cinco (5) años de experiencia en el área.

Capacitaciones, cursos y/o seminarios recibidos:

- ISO 27001 2022
- Lead Implementer
- Foundation
- Lead Auditor
- CEHPC
- Hacking Ético

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. 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.
7. Supervisar y administrar el acceso a sistemas y datos confidenciales, asegurando que solo personal autorizado tenga permisos adecuados.
8. Establecer y dar seguimiento continuo a los controles de seguridad, como firewalls, sistemas de detección de intrusiones (IDS), WAF, XDR, NDR, DLP, CISCO Umbrella/DNS, gestión de vulnerabilidades y cifrado, para garantizar la protección y resiliencia de la infraestructura tecnológica.
9. Responder a incidentes de seguridad, investigar incidentes de seguridad y aplicar medidas correctivas.
10. Administrar y mejorar las herramientas de protección perimetral y monitoreo continuo (SIEM, XDR, NDR, CISCO Umbrella, DLP, etc.).
11. Gestionar la seguridad en infraestructura híbrida, incluyendo entornos de nube pública y privada, asegurando su correcta configuración y cumplimiento.
12. Ejecutar análisis de vulnerabilidades, aplicar remediaciones técnicas y mantener actualizados los sistemas según los hallazgos.
13. Completar y reportar los KPI de ciberseguridad operativa, incluyendo métricas de incidentes, vulnerabilidades, accesos, entre otros.
14. Gestionar el ciclo de vida de usuarios y accesos, incluyendo la creación, modificación, y baja de cuentas, garantizando que los accesos sean asignados de acuerdo con el rol, revisados periódicamente y eliminados cuando ya no sean necesarios.
15. Crear, actualizar y documentar lecciones aprendidas tras incidentes, asegurando su uso en la mejora continua de los controles.

La SIECA cuenta con triple certificación en Sistemas de Gestión.

Para más información visite www.sieca.int

4ª avenida 10-25 zona 14, Ciudad de Guatemala, Centroamérica. 01014





16. Monitorear fuentes de inteligencia de amenazas (feeds, ISACs, herramientas automatizadas, etc.) para anticiparse a riesgos emergentes y adaptar los controles de seguridad.
17. Investigar y analizar continuamente la superficie de ataque de la organización, identificando activos expuestos, servicios mal configurados y puntos débiles en sistemas internos, en la nube o en la red pública, para proponer medidas de mitigación proactiva.
18. Ejecución de pruebas de penetración (pentesting) para evaluar vulnerabilidades y fortalecer los controles de seguridad.

Experiencia laboral mínima comprobable:

Cinco años (5) de experiencia comprobable en ciberseguridad operativa, seguridad de la información incluyendo administración de controles de seguridad, gestión de vulnerabilidades, monitoreo de amenazas, respuesta a incidentes, administración de accesos y protección de infraestructura tecnológica híbrida o en la nube.

Se valorará experiencia en el uso de herramientas como SIEM, XDR, NDR, DLP, WAF, IDS/IPS, firewalls y soluciones de seguridad DNS, así como en auditorías de seguridad, documentación técnica y seguimiento de indicadores operativos.

Requisitos deseables:

- Experiencia en la implementación y gestión de sistemas de gestión de seguridad de la información (SGSI) bajo normativas: ISO/IEC 27001.
- Experiencia en la gestión de herramientas de ciberseguridad como firewalls, IDS/IPS, SIEM, XDR, NDR, DLP, etc.
- Experiencia en la gestión de seguridad en entornos híbridos, tanto en la nube pública como privada.
- Experiencia en la ejecución de análisis de vulnerabilidades y remediación de problemas técnicos.
- Conocimiento en la administración de herramientas de protección perimetral y monitoreo continuo (SIEM, XDR, DLP, etc.).
- Capacidad para gestionar y monitorear accesos a sistemas, aplicar políticas de gestión de identidades y controlar accesos.
- Capacidad para realizar análisis forenses y de incidentes de seguridad, con enfoque en la mejora continua de los controles.
- Experiencia en la implementación de medidas de mitigación frente a amenazas emergentes y nuevos vectores de ataque.
- Conocimiento sobre configuración segura de infraestructura en la nube y protección de datos.
- Conocimiento de mejores prácticas de ciberseguridad (NIST, CIS Controls, etc.) y normativas relevantes para la infraestructura tecnológica.
- Experiencia en la administración de seguridad perimetral (firewalls, IDS/IPS) y gestión de sistemas SGSI bajo ISO/IEC 27001. Conocimiento en la gestión de riesgos, auditorías internas, planes de continuidad de negocio y herramientas de ciberseguridad (SIEM, XDR, DLP). Participación en procesos de certificación ISO 20000-1 y 27001.

Habilidades básicas, técnicas, otras:

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

Competencias técnicas:

A nivel 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.

A nivel de dominio:

- Fundamentos de seguridad, tecnologías de red, sistemas operativos, criptografía, gestión de identidad, seguridad de aplicaciones y protocolos.

INFORMACIÓN IMPORTANTE:

Lineamientos para aplicar como postulante:

1. Leer detenidamente la convocatoria y seguir minuciosamente las instrucciones que allí se indican.
2. Descargar, completar e incorporar los formatos adjuntos en la convocatoria (ubicados en la página web de la SIECA) como parte de su postulación.

La SIECA cuenta con triple certificación en Sistemas de Gestión.

Para más información visite www.sieca.int

4ª avenida 10-25 zona 14, Ciudad de Guatemala, Centroamérica. 01014





3. La postulación debe ser remitida a la casilla electrónica reclutamientos@sieca.int con copia al correo msoto@sieca.int adjuntando la siguiente información obligatoria **DENTRO DE UN SOLO DOCUMENTO en formato PDF Y EN EL ORDEN QUE SE MUESTRA A CONTINUACIÓN:**
 - Hoja de vida actualizada, incorporando la siguiente información básica:
 - Datos personales: Compuesta por nombre completo, domicilio, teléfono, edad, fecha de nacimiento, nacionalidad.
 - Formación académica: Plasmada de forma descendente (del año más reciente al año más antiguo), especificando fecha de inicio y de fin, grado alcanzado, casa de estudios, país.
 - Experiencia laboral: Plasmada de forma descendente (del año más reciente al año más antiguo), especificando puesto desempeñado, fecha de inicio y de fin (mes/año), funciones realizadas, institución y país.
 - Referencias laborales: Cada una debe estar estructurada de la siguiente manera:
 - ✓ Institución en la que laboró
 - ✓ Puesto desempeñado
 - ✓ Período de ejecución
 - ✓ Jefatura inmediata
 - ✓ Puesto de Jefatura inmediata
 - ✓ Teléfono personal de Jefatura inmediata
 - 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)
 - Título(s) universitario(s) de grado y/o pregrado, cierre(s) de pñsum universitario, certificado de notas del último grado universitario aprobado, título(s) a nivel diversificado (según aplique con base a lo requerido para la vacante; deben ser anexados dentro de un mismo documento).
 - Constancias de cursos recibidos (según aplique con base a lo requerido para la vacante; deben ser anexados dentro de un mismo documento).
4. La postulación debe ser remitida **a más tardar el 15 de octubre del año 2026 a las 23:59** horas, ya que, posterior a ello no será considerada.

Observaciones:

1. 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.
2. 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).
3. 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.
4. En casos debidamente calificados o justificados, podrán participar personas de otras nacionalidades en los procesos de contratación de la SIECA.

