



NOMBRE DEL(LA) POSTULANTE: _____

CUADRO CON INFORMACIÓN PROFESIONAL COMPLEMENTARIA

VACANTE: ADMINISTRADOR: SEGURIDAD INFORMÁTICA

Nro.	Aspectos importantes:	Sí/No	Información adicional
1.	Esta vacante es de tipo indefinido (bajo nómina/planilla), la modalidad de labores del puesto es 100% presencial en la Ciudad de Guatemala (no híbrida, ni remota). Las funciones del puesto vacante se desempeñarán presencialmente en la Secretaría de Integración Económica Centroamericana (SIECA) ubicada en la dirección: 4ª avenida, 10-25 zona 14, Ciudad de Guatemala, Guatemala. El postulante interesado, tendrá claro que, de ser seleccionado para ocupar la vacante, deberá trasladarse y residir por cuenta propia en el país sede de la SIECA (Guatemala), en caso de tener residencia fuera de los límites territoriales de dicho país. ¿Está de acuerdo con la metodología y el traslado de residencia en caso de ser necesario?		
2.	¿Su pretensión salarial es negociable? En caso de sí serlo, complete los recuadros contiguos, especificando el monto salarial mínimo negociable (en dólares de USA) que está dispuesto(a) a aceptar.		Favor indicar la cantidad en DÓLARES hasta la cual sería negociable su pretensión salarial:
3.	Estudiante de las carreras de Ingeniería en Sistemas, Licenciatura en Informática, carrera afín o cinco (5) años de experiencia en el área. En caso afirmativo, complete los recuadros contiguos, especificando su especialidad, último grado aprobado y grado activo.		





Nro.	Preguntas en torno a experiencia laboral:	Sí/No	Puesto en el que ejecutó la experiencia (desarrolle/detalle)	Tiempo de experiencia alcanzado (en años)	Empresa/ Institución
4.	¿Cuenta con 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 nube?				
5.	¿Cuenta con 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? ¿Cuántos meses o años?				
6.	¿Ha cumplido con las políticas, lineamientos y disposiciones establecidos en los diferentes manuales administrativos y normativas de la institución o empresa para la que ha trabajado, así como de los Proyectos de Cooperación cuando aplique, según el convenio de cooperación?				
7.	¿Ha identificado y evaluado riesgos de seguridad, y desarrollar estrategias para mitigarlos?				
8.	¿Ha actualizado amenazas y tecnologías de seguridad de al menos los últimos 3 meses, implementando actualizaciones y mejoras según sea necesario?				
9.	¿Ha trabajado en estrecha colaboración con otras áreas de la institución para la que ha trabajado, para garantizar la integración de la seguridad en todas las áreas de la organización?				
10.	¿Ha acompañado junto con la dirección o unidad responsable de las auditorías externas e internas del sistema de gestión de seguridad de la información?				
11.	¿Ha realizado 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?				
12.	¿Ha supervisado y administrado el acceso a sistemas y datos confidenciales, asegurando que solo personal autorizado tenga permisos adecuados?				



13.	¿Ha establecido 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?				
14.	¿Ha respondido a incidentes de seguridad, investigado incidentes de seguridad y aplicado medidas correctivas?				
15.	¿Ha administrado y mejorado las herramientas de protección perimetral y monitoreo continuo (SIEM, XDR, NDR, CISCO Umbrella, DLP, etc.)?				
16.	¿Ha gestionado la seguridad en infraestructura híbrida, incluyendo entornos de nube pública y privada, asegurando su correcta configuración y cumplimiento?				
17.	¿Ha ejecutado análisis de vulnerabilidades, aplicado remediaciones técnicas y mantenido actualizados los sistemas según los hallazgos?				
18.	¿Ha completado y reportar los KPI de ciberseguridad operativa, incluyendo métricas de incidentes, vulnerabilidades, accesos, entre otros?				
19.	¿Ha gestionado 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?				
20.	¿Ha creado, actualizado y documentado lecciones aprendidas tras incidentes, asegurando su uso en la mejora continua de los controles?				
21.	¿Ha monitoreado fuentes de inteligencia de amenazas (feeds, ISACs, herramientas automatizadas, etc.) para anticiparse a riesgos emergentes y adaptar los controles de seguridad?				
22.	¿Ha investigado y analizado 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?				





23	¿Ha ejecutado pruebas de penetración (pentesting) para evaluar vulnerabilidades y fortalecer los controles de seguridad?				
----	--	--	--	--	--

CAPACITACIONES, CURSOS, SEMINARIOS, TALLERES, ETC. (OBLIGATORIO)				
Nro.	Temática	Sí/No	Nivel adquirido (básico/intermedio/ avanzado)	Cuenta con certificado que lo respalde (Sí /No)
1.	ISO 27001 2022			
2.	Lead Implementer			
3.	Foundation			
4.	Lead Auditor			
5.	CEHPC			
6.	Hacking Ético			

HABILIDADES Y COMPETENCIAS TÉCNICAS (OBLIGATORIA)				
Nro.	HABILIDADES	Sí/No	Nivel de manejo adquirido (básico/intermedio/ avanzado)	Cuenta con certificado que lo respalde (Sí /No)
1.	¿Con qué nivel de dominio posee del idioma extranjero/inglés'?			
2.	¿Con qué manejo de paquete de programas informáticos de Microsoft Office y otras herramientas de gestión virtual?			
Nro.	COMPETENCIAS (a nivel de conocimiento)	Sí/No	Nivel de conocimiento adquirido (básico/intermedio/ avanzado)	Cuenta con certificado que lo respalde (Sí /No)
3.	Normativa ISO/IEC 20000-1 e ISO/IEC27001			
4.	Entender leyes y normativas, estar actualizado en herramientas de seguridad y desarrollar habilidades en la gestión de incidentes.			
Nro.	COMPETENCIAS (a nivel de dominio)	Sí/No	Nivel de dominio adquirido (básico/intermedio/ avanzado)	Cuenta con certificado que lo respalde (Sí /No)
5.	Fundamentos de seguridad, tecnologías de red, sistemas operativos, criptografía, gestión de identidad, seguridad de aplicaciones y protocolos.			





REQUISITOS DESEABLES

Nro.	Experiencia laboral	Sí/No	Puesto en el que ejecutó tal experiencia	Tiempo de experiencia en años	Empresa/ Institución
1.	Experiencia en la implementación y gestión de sistemas de gestión de seguridad de la información (SGSI) bajo normativas: ISO/IEC 27001.				
2.	Experiencia en la gestión de herramientas de ciberseguridad como firewalls, IDS/IPS, SIEM, XDR, NDR, DLP, etc.				
3.	Experiencia en la gestión de seguridad en entornos híbridos, tanto en la nube pública como privada.				
4.	Experiencia en la ejecución de análisis de vulnerabilidades y remediación de problemas técnicos.				
5.	Conocimiento en la administración de herramientas de protección perimetral y monitoreo continuo (SIEM, XDR, DLP, etc.).				
6.	Capacidad para gestionar y monitorear accesos a sistemas, aplicar políticas de gestión de identidades y controlar accesos.				
7.	Capacidad para realizar análisis forenses y de incidentes de seguridad, con enfoque en la mejora continua de los controles.				
8.	Experiencia en la implementación de medidas de mitigación frente a amenazas emergentes y nuevos vectores de ataque				
9.	Conocimiento sobre configuración segura de infraestructura en la nube y protección de datos.				
10.	Conocimiento de mejores prácticas de ciberseguridad (NIST, CIS Controls, etc.) y normativas relevantes para la infraestructura tecnológica.				
11.	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.				

