NOMBRE DEL(LA) POSTULANTE:

CUADRO CON INFORMACIÓN PROFESIONAL COMPLEMENTARIA – ADMINISTRADOR "B": SEGURIDAD INFORMÁTICA			
Nro.	**Preguntas importantes:**	**Sí/No**	**Información adicional**
1.	Esta vacante es de tipo indefinido (bajo nómina/planilla), la modalidad de labores del puesto es 100% presencial (**no híbrida ni remota).** Las funciones del puesto se desempeñarán en la Secretaría de Integración Económica Centroamericana (SIECA) con dirección: 4ª avenida, 10-25 zona 14, Ciudad de Guatemala, Guatemala. El interesado debe estar claro que, en caso de ser seleccionado para ocupar la vacante, deberá trasladarse y residir por cuenta propia en el país sede de la SIECA (Guatemala). ¿Está de acuerdo con la metodología y el traslado de residencia en caso de ser necesario?		
2.	¿Su aspiración salarial es negociable? En caso de sí serlo, complete los recuadros contiguos, especificando la cantidad mínima negociable en dólares que está dispuesto a aceptar.		

Nro.	Preguntas importantes:	Sí/No	Información adicional		
3.	¿Es estudiante del último año de las carreras de Ingeniería en Sistemas, Licenciatura en Informática, o carreras afines?				
4.	En caso de no contar con el requisito anterior, ¿cuenta con cinco (05) años de experiencia en puestos similares al de la vacante (con especialización en Seguridad Informática)?				
Nro.	**Preguntas en torno a experiencia laboral:**	**Sí/No**	**Puesto en el que ejecutó tal experiencia**	**Tiempo de experiencia en años**	**Empresa/ Institución**
5.	¿Cuenta con dos (02) años en puestos similares, gestionando políticas y procedimientos de seguridad informática y participando en procesos de auditoría de seguridad de información? (tiempo aceptado si se cumple con el requisito académico)				
6.	¿Ha cumplido con las políticas, lineamientos y disposiciones establecidos en los diferentes manuales administrativos y normativas de las instituciones en las que ha laborado?				
7.	¿Ha identificado y evaluado riesgos de seguridad, y ha desarrollado estrategias para mitigarlos?				
8.	¿Se ha actualizado de las últimas amenazas y tecnologías de seguridad de al menos los últimos 3 meses, implementando actualizaciones y mejoras según sea necesario?				

Nro.	Preguntas en torno a experiencia laboral:	Sí/No	Puesto en el que ejecutó tal experiencia	Tiempo de experiencia en años	Empresa/ Institución
9.	¿Ha trabajado en estrecha colaboración con otras áreas y/o departamentos, para garantizar la integración de la seguridad en todas las áreas de las instituciones en las que ha laborado?				
10.	¿Ha brindado acompañamiento junto con la dirección o unidad responsable de las auditorías externas e internas del sistema de gestión de seguridad de la información?				
11.	¿Ha creado y mantenido políticas y procedimientos de seguridad de la información alineados a la normativa ISO/IEC 27001:2022?				
12.	¿Ha implementado y dado seguimiento al cumplimiento de controles y proyectos de ciberseguridad?				
13.	¿Ha coordinado y respondido a incidentes de seguridad, investigar incidentes y asegurar que las medidas correctivas sean eficaces?				
14.	¿Ha impartido programas de concientización sobre seguridad y proporcionar capacitación regular para el personal de la empresa?				
15.	¿Ha planificado, ejecutado y evaluado campañas internas de pruebas de phishing, analizando los resultados y ajustando los programas de				

	concientización y capacitación según los hallazgos obtenidos?				
Nro.	**Preguntas en torno a experiencia laboral:**	**Sí/No**	**Puesto en el que ejecutó tal experiencia**	**Tiempo de experiencia en años**	**Empresa/ Institución**
16.	¿Ha liderado 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?				
17.	¿Ha desarrollado, implementado y mantenido 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?				
18.	¿Ha realizado auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad y los estándares establecidos?				
19.	¿Ha dado 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?				

Nro.	Preguntas en torno a experiencia laboral:	Sí/No	Puesto en el que ejecutó tal experiencia	Tiempo de experiencia en años	Empresa/ Institución
20.	¿Ha asegurado la implementación adecuada de controles de seguridad física y lógica para proteger los activos de información?				
21.	¿Ha asegurado 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?				
22.	¿Ha dado seguimiento y análisis a los KPI de ciberseguridad para evaluar el desempeño y efectividad de las actividades y controles implementados?				

HABILIDADES BÁSICAS Y COMPETENCIAS TÉCNICAS				
Nro.	**Cuenta con los siguientes aspectos**	**Sí/No**	**Nivel de conocimiento y/o dominio adquirido (no tiene/básico/intermedio/ avanzado)**	**Cuenta con certificado que lo respalde (Sí /No)**
1.	Manejo avanzado de paquete de programas informáticos de Microsoft Office y otras herramientas de gestión virtual			
2.	Nivel intermedio del idioma inglés			
3.	Entender leyes y normativas de seguridad.			
4.	Estar actualizado en herramientas de seguridad.			

5.	Desarrollar habilidades en la gestión de incidentes.			
6.	Fundamentos de seguridad			
7.	Tecnologías de red			
8.	Sistemas operativos			
9.	Criptografía			
10.	Gestión de identidad			
11.	Seguridad de aplicaciones y protocolos			
12.	Conocimiento de las normativas ISO 20000-1.			
13.	Conocimiento de las normativas ISO 27001.			
14.	Experiencia en la implementación y gestión de sistemas de gestión de seguridad de la información (SGSI) bajo normativas: ISO/IEC 27001.			
15.	Conocimientos y experiencia práctica en la gestión de riesgos de seguridad de la información y auditorías internas.			
16.	Experiencia en la planificación y ejecución de planes de continuidad de negocio y recuperación ante desastres.			
17.	Conocimiento avanzado en políticas de seguridad, controles de seguridad física y lógica, y gestión de riesgos			

18.	Capacidad para diseñar e implementar programas de concientización y capacitación en seguridad informática. Experiencia en la implementación de controles de ciberseguridad, como protección de datos y medidas de protección perimetral.			

CURSOS, SEMINARIOS, TALLERES, ETC.				
Nro.	**¿Ha realizado cursos, seminarios, talleres, etc. sobre los siguientes temas?**	**Sí/No**	**Nivel de conocimiento y/o dominio adquirido (no tiene/básico/intermedio/ avanzado)**	**Cuenta con certificado que lo respalde (Sí /No)**
1.	Análisis Forense digital / Informática forense			
2.	ISO 27001			
3.	ISO 20000-1			
4.	Ethical Hacking			
5.	Análisis de vulnerabilidades			
6.	Protocolos de seguridad (IPSec)			