NOMBRE DEL(LA) POSTULANTE:_____

CUADRO CON INFORMACIÓN PROFESIONAL COMPLEMENTARIA Administrador Junior Seguridad Informática			
Nro.	**Preguntas importantes:**	**Sí/No**	**Información adicional**
1.	Esta posición es de carácter indefinido (bajo nómina/planilla), la modalidad de labores del puesto es 100% presencial (**no híbrida ni remota)** en la ciudad de Guatemala. Si fuera seleccionado(a) para ocupar la vacante, deberá trasladarse y vivir por su cuenta en Guatemala (en caso de residir fuera de los límites de dicho país). ¿Estaría de acuerdo con la metodología y el traslado de país en caso de ser necesario?		
2.	¿Su aspiración salarial es negociable? En caso de sí serlo, complete los recuadros contiguos, especificando la cantidad negociable en dólares.		
3.	¿Es estudiante del último año de las carreras de Ingeniería en Sistemas, Licenciatura en Informática, carrera afín o 5 años de experiencia en el área.? En caso afirmativo complete los recuadros contiguos, especificando el grado alcanzado, si se encuentra activo y, de ser así, el grado en curso.		

4.	¿Cuenta con especialización en Seguridad Informática?				
5.	¿Tiene dos años en puestos similares, gestionando políticas y procedimientos de seguridad informática y participando en procesos de auditoría de seguridad de información?.				

Nro.	Preguntas en torno a experiencia laboral:	Sí/No	Puesto en el que ejecutó tal experiencia	Tiempo de experiencia en años	Empresa/ Institución
6.	¿ Dos años en puestos similares, gestionando políticas y procedimientos de seguridad informática y participando en procesos de auditoría de seguridad de información? (especifique)?				
7.	¿Ha identificado y evaluado riesgos de seguridad, y desarrollar estrategias para mitigarlos?				
8.	¿Ha mantenido actualizado de las últimas 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 direcciones del lugar donde ha laborado, 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 creado y mantenido políticas y procedimientos de seguridad de la información alineados a la normativa ISO/IEC 27001:2022?				
12.	¿Ha implementado y dado cumplimiento de controles y proyectos de ciberseguridad.?				
12.	¿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?				
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? ¿Ha realizado auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad y los estándares establecidos?				
18.	¿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?				
19.	¿Ha asegurado la implementación adecuada de controles de seguridad física y lógica para proteger los activos de información?				
20.	¿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 dato?				
21.	¿Ha dado seguimiento y análisis a los KPI de ciberseguridad para evaluar el desempeño y efectividad de las actividades y controles implementados?				

Requisitos deseables, favor completar si cuenta con el conocimiento:

Nro.	Preguntas en torno a experiencia laboral:	Sí/No	Puesto en el que ejecutó tal experiencia	Tiempo de experiencia en años	Empresa/ Institución
1.	Tiene Experiencia en la implementación y gestión de sistemas de gestión de seguridad de la información (SGSI) bajo normativas: ISO/IEC 27001?				
2.	Tiene 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.	Tiene experiencia en la implementación de controles de ciberseguridad, como protección de datos y medidas de protección perimetral?				

Nro.	Preguntas sobre habilidades, técnicas, etc.	Sí/No	Nivel de conocimiento 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.	Conoce la Normativa ISO/IEC 20000-1 e ISO/IEC27001?			
4.	Entiende de leyes y normativas, estar actualizado en herramientas de seguridad y desarrollar habilidades en la gestión de incidentes?			
5.	Tiene Fundamentos de seguridad, tecnologías de red, sistemas operativos, criptografía, gestión de identidad, seguridad de aplicaciones y protocolos?			
6.	Tiene 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?			

Nro.	¿Ha recibido capacitaciones, cursos, diplomados y/o seminarios sobre los siguientes temas?	Sí/No	Nivel de conocimiento o dominio adquirido (no tiene/básico/intermedio/ avanzado)	Cuenta con certificado que lo respalde (Sí /No)
1.	Análisis Forense, ISO 27001, Ethical Hacking, Análisis de vulnerabilidades, Protocolos de seguridad (IPSec)?			
2.	Capacitaciones sobre trabajo en equipo, relaciones humanas, administración del tiempo, manejo de estrés laboral?			