Concurso Externo Nº 07-2025

De conformidad con autorización que consta en los oficios BANHVI-GG-OF-1028-2024, la Dirección Administrativa y el Área de Recursos Humanos convocan a los interesados al **Concurso Externo** para ocupar los siguientes puestos:

I. Características del puesto.

- **Puesto:** Analista de Sistemas Encargado Seguridad TI
- **Categoría:** 11
- **Puesto:** 929
- **Tipo de nombramiento**: Nombramiento en plaza fija (con periodo de prueba)
- **Salario del puesto:** ¢1,272,062.38
- **Dependencia:** Departamento de Tecnología de Información

II. Temas preliminares:

a) Procedimiento: El concurso se realizará de conformidad con el Procedimiento de Dotación de Personal: (PA-GRH-CP-PR01), en lo que aquí interesa, se aplicará las siguientes cuatro fases, asignándose una ponderación en una base de 100 de acuerdo con la siguiente tabla:

FASE	PONDERACIÓN
1) Evaluación de requisitos	20%
2) Evaluación de la idoneidad	30%
3) Verificación de referencias	n/a*
4) Entrevista	50%

* Esta fase no tiene ponderación asociada, pero de presentar alguna inconsistencia el postulante no podrá pasar a la etapa siguiente.

b) Requisitos Indispensables: Los interesados en participar, deberán llenar y firmar la declaración jurada adjunta, haciendo constar que cumplen los requisitos indispensables para ocupar esta posición. estos requisitos son los de admisibilidad según el perfil del puesto.

El candidato que no los cumpla o no presente la declaración jurada, quedará automáticamente descalificado.

- ☑ Licenciatura en Computación o Informática
- ☑ Conocimientos en Bases de Datos, Infraestructura, Telecomunicaciones.
- ☑ Al menos 3 años de experiencia en labores relacionadas con la Seguridad de TI, analizando y/o gestionando los siguientes dominios de seguridad:
  - Seguridad de la Información y validación de Riesgos relativos a vulnerabilidades de Seguridad de TI.
  - Sistemas y Metodologías de Control de Acceso.
  - Seguridad Física.
  - Arquitectura y Diseño de Seguridad.
  - Legislación, Regulaciones y Cumplimiento Normativo, relativos a la Seguridad de TI.
  - Seguridad de redes y Telecomunicaciones.
  - Planes de continuidad del negocio y de Recuperación Frente a Desastres.
  - Seguridad de las Aplicaciones.

- Seguridad de los esquemas de servicios sobre Internet/Intranet.
- Seguridad y Autenticidad de los servicios sobre de correo electrónico.
- Seguridad sobre los mecanismos para el trasiego o transferencia de información vital y confidencial.

☑ Manejo de inglés técnico (Lectura y comprensión a nivel alto).
☑ Conocimientos de ITIL.
☑ Conocimientos de COBIT.
☑ Manejo de Software utilizado para Talleres de Ethical Hacker.
☑ Conocimiento del modelo de Análisis de Riesgos de TI de ISACA.
☑ Conocimiento del Estándar para seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements).
☑ Conocimiento del Estándar para la seguridad de la información ISO/IEC 27002 (anteriormente referenciado como ISO/IEC 17799).
☑ Conocimiento del Reglamento General de Gestión de la Tecnología de Información de la SUGEF, vigente.
☑ Conocimiento de las Normas Técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República, vigente.
☑ Conocimiento en plataformas como Active Directory, SQL SERVER, Oracle, Redes LAN, Redes WAN y Cloud Computing.
☑ Capacidad para investigar y leer material técnico y de negocios relacionado con el tema de Riesgos de TI.

III. **Fases Evaluables:**

A) Evaluación de requisitos (20%): Según el desglose presentado en la siguiente tabla, serán evaluados los siguientes requisitos:

Criterios de evaluación	Puntaje	Ponderación máxima
1. Formación académica:		**5%**
1.1 Licenciatura en Computación o Informática	5 %	
2. Experiencia laboral: Para validar la experiencia laboral específica el participante deberá presentar la constancia de tiempo servido en la que detalle: institución, tiempo servido, puesto desempeñado y descripción de funciones. En caso de que la constancia no detalle la descripción de funciones, podrá presentar la descripción del puesto.		**40%**
2.1 Al menos 3 años de experiencia en labores relacionadas con la Seguridad de TI, analizando y/o gestionando los siguientes dominios de seguridad: • Seguridad de la Información y validación de Riesgos relativos a vulnerabilidades de Seguridad de TI. • Sistemas y Metodologías de Control de Acceso. • Seguridad Física. • Arquitectura y Diseño de Seguridad. • Legislación, Regulaciones y Cumplimiento Normativo, relativos a la Seguridad de TI. • Seguridad de redes y Telecomunicaciones. • Planes de continuidad del negocio y de Recuperación Frente a Desastres. • Seguridad de las Aplicaciones. • Seguridad de los esquemas de servicios sobre Internet/Intranet. • Seguridad y Autenticidad de los servicios sobre de correo electrónico. • Seguridad sobre los mecanismos para el trasiego o transferencia de información vital y confidencial.	10%	
2.2 De 3 años y un día hasta 4 años	25%	
2.3 De 4 años en adelante	40%	

3. Áreas de conocimiento requeridos: Para validar los conocimientos el participante deberá presentar certificados o constancia de tiempo servido en la que detalle: institución, tiempo servido, puesto desempeñado y descripción de funciones. En caso de que la constancia no detalle la descripción de funciones, podrá presentar la descripción del puesto respectivo.	55%	**55%**
3.1 Conocimientos en Bases de Datos, Infraestructura, Telecomunicaciones.	5%	
3.2 Conocimientos de ITIL	5%	
3.3 Conocimientos de COBIT	5%	
3.4 Manejo de Software utilizado para Talleres de Ethical Hacker	5%	
3.5 Conocimiento del Estándar para seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements).	5%	
3.6 Conocimiento del Estándar para la seguridad de la información ISO/IEC 27002 (anteriormente referenciado como ISO/IEC 17799).	5%	
3.7 Conocimiento del Reglamento General de Gestión de la Tecnología de Información de la SUGEF, vigente	5%	
3.8 Conocimiento de las Normas Técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República, vigente	5%	
3.9 Conocimiento en plataformas como Active Directory, SQL SERVER, Oracle, Redes LAN, Redes WAN y Cloud Computing	5%	
3.10 Capacidad para investigar y leer material técnico y de negocios relacionado con el tema de Riesgos de TI.	5%	
3.11 Manejo de inglés técnico (Lectura y comprensión a nivel alto).	5%	
Total	100	**100%**

Para que un postulante supere esta fase, es requisito indispensable que alcance un resultado mínimo de 70 puntos, de esta manera pasará a la siguiente fase.

B) Aplicación de prueba de idoneidad (30%)

Los candidatos que superen la nota mínima señalada en el punto A) anterior, serán contactados para la aplicación de una prueba técnica.

En dicha prueba se evaluarán conocimientos en los siguientes temas:

- Seguridad de la Información y Gestión de Riesgos
- Control de Acceso y Seguridad Física
- Cumplimiento Normativo y Legislación en Seguridad de TI
- Seguridad de Redes y Telecomunicaciones
- Planes de Continuidad del Negocio y Recuperación ante Desastres
- Seguridad de Aplicaciones y Servicios en Internet

C) Verificación de referencias: personales, laborales, legales, patrimoniales y política conflicto de intereses.

Se procederá con la verificación de las referencias que fueron suministradas por el postulante al llenar los formularios de la oferta de servicios y de información socioeconómica y la verificación de la Política de Conflicto de Interés PO-INS-CIN-001, según la cual se considera una situación generadora de conflicto de interés el estar vinculado durante el último año con alguna empresa proveedora de servicios al Banco que esté directamente relacionada con el proyecto para el cual estará laborando, entre otros alcances de esa misma política.

D) Entrevista (50%)

Los postulantes que superen con éxito las etapas previas, incluida la verificación de las referencias, serán convocados a entrevista. La nota mínima de la entrevista es de 70 puntos.

E) Registro de elegibles:

Los candidatos que no resultaron seleccionados y obtuvieron una ponderación mínima de 70 puntos, pasarán a formar parte del registro de elegibles por un periodo de un año, para posiciones que tengan la misma categoría y especialidad.

De conformidad con las bases del concurso, los candidatos interesados en participar deberán enviar la documentación solicitada a la siguiente dirección de correo electrónico: hr3@dorispeters.com

Fecha límite de inscripción: 31/03/2025.

MARGOT CAMPOS BARRANTES (FIRMA)

Firmado digitalmente por MARGOT CAMPOS BARRANTES (FIRMA)
Fecha: 2025.03.19 09:47:44 -06'00'

MBA. Margoth Campos Barrantes
Dirección Administrativa