



## GENERAL SECRETARIAT OF THE ORGANIZATION OF AMERICAN STATES

Secretariat for Administration and Finance (SAF)  
Department of Information and Technology Services (DOITS)

### CALL FOR RESUME

**Type of contract:** Consultant

**Field:** Information Security Engineer

**Location:** Remote or Headquarters

**Start date:** TBD

**Deadline for Application:** March 24, 2025

**Remuneration Range:** Based on experience, education, location, and skills

Consultancy opportunity number: CFR/12/25

The Department of Information and Technology Services is responsible for managing all Systems and Technology infrastructure resources and personnel, including all matters related to the plans, policies, procedures and standards governing the utilization of technology resources and management of information technology services of the General Secretariat of the OAS

Candidates will be responsible for technical aspects related to Security Systems implemented at the GS/OAS. The main role is to provide hands-on operational capabilities to the GS/OAS Information Security Architecture. Operations activities include successfully maintaining network security appliances, perimeter security systems, cloud-based security controls, and on-premises security infrastructure, along with the associated documentation, diagrams, and procedures. Additionally, the Information Security Engineer is responsible for the installation, configuration, maintenance, and upgrade of both cloud and on-premises information security systems.

### DUTIES AND ACCOUNTABILITIES

The areas of concentration encompass the following fields:

- Security penetration research, information security diagnostic review, information security architecture and design, security software evaluation and selection, application security review, risk assessment, and data classification.

- Assist in the development of security-related policies, procedures, and standards.
- Maintain and manage internet security devices and network security.
- Support the CISO in all technical aspects regarding investigations of security breaches related to IT infrastructure and information.
- Aid in enforcing policies related to the use of digital information resources, security of wireless systems, remote access to the organization's network, and digital interaction with OAS offices, missions, partner organizations, and local businesses.
- Utilize information security tools to prepare reports evaluating the organization's security posture.
- Monitor OAS IT infrastructure, identify new threats and vulnerabilities, and recommend security solutions.
- Develop tools and processes to help evaluate contingency requirements and priorities for information systems.
- Provide guidance to identify business practices dependent on IT systems that could affect primary organizational functions during incidents.
- Test and evaluate new products and technologies; prepare various technical reports.
- Oversee adherence to information security policies and procedures.
- Support GS/OAS information security architecture, including servers, software, and associated hardware.
- Develop procedures and strategies for information security administration and maintenance; create and maintain comprehensive documentation for all implemented security solutions.
- Research and recommend information security solutions to meet growing organizational requirements.
- Provide feedback on the effectiveness of implemented security products through reports and recommendations.
- Attend team meetings with senior technical staff to coordinate work and solve emerging problems.
- When assigned project manager responsibility, manage the project by:
  - Developing the project plan.
  - Estimating and directing resources.
  - Monitoring and managing the project schedule, budget, and risks.
  - Engaging and maintaining communication with stakeholders.
  - Reporting to the CISO and other relevant officials on strategic issues.
  - Preparing project status reports and documentation.
  - Ensuring the project meets requirements and objectives.

## **REQUIREMENTS**

### **Essential:**

### **Education:**

- Bachelor's Degree in Computer Science, Computer Engineering, or a related field.

### **Language Requirements:**

- Excellent oral, written, and communication skills in English and Spanish.

### **Professional Experience:**

- 2+ years of progressively responsible experience implementing and administering information security solutions.
- 4+ years of progressively responsible experience implementing security projects and solutions, including the deployment of security technologies, developing security strategies, and maintaining secure systems.

- Training and experience in planning, designing, installing, and maintaining information security solutions.
- Experience with open-source information security solutions.
- Thorough knowledge of network operating systems and protocols, Linux and Windows environments, and network manager applications.

**Desirable:**

- ITIL certification or familiarity with ITIL practices.
- Advanced University Degree (Master's) in Information Security.
- CISSP or similar certifications.
- Project management certification.
- Knowledge of SIEM platforms.
- Experience with risk management and compliance.
- Experience with Azure cloud security.
- Experience with vulnerability management tools and methodologies.
- Experience managing cloud security solutions.
- Familiarity with Microsoft Purview.
- Strong background in project management, including coordinating across diverse teams and stakeholders.

**SUBMISSION OF APPLICATIONS:**

Interested candidates should send their CV and cover letter (no more than 250 words) with the subject "Information Security Support" to [DOITS-CV@oas.org](mailto:DOITS-CV@oas.org)

No phone inquiries accepted. Only shortlisted candidates will be contacted.

**The GS/OAS embraces equality, diversity, and inclusion. Thus, the GS/OAS, in accordance with its rules and regulations, is committed to providing equal opportunities in employment, achieving a diverse staff, and will consider a wide geographic representation, as well as gender equity and equality, in the selection of candidates.**