INAGE,IP
Instituto Nacional de Governo Electrónico, Instituto Público

DIVISÃO DE SEGURANÇA CIBERNÉTICA

Equipa de Resposta a Incidentes de Segurança Cibernética do Governo

CSIRT.GOV

RFC 2350

Maputo, Julho de 2025

1. Information About This Document

This document describes the cybersecurity incident response service of the **Government Cybersecurity Incident Response Team (CSIRT.GOV)**, according to the **RFC 2350**.

1.1. Date of Last Update

- Version 1.1 published on 2025/07/14
- Version 1.2 – Update of CSIRT links and services on 2025/10/23
- Monday, July 14th, 12:59:15 (GMT +2)

1.2. Distribution List for Notifications

There is no existing distribution channel for notifications of updates.

1.3. Access to This Document

The Portuguese version of this document is available at:

https://csirt.gov.mz/wp-content/uploads/2025/10/RFC-2350.pdf

The English version of this document is available at:

https://csirt.gov.mz/wp-content/uploads/2025/10/RFC-2350-En.pdf

1.4. Authenticity of This Document

This document is signed with the PGP key of **CSIRT.GOV**.

2. Contact Information

2.1. Team Name

Government Cybersecurity Incident Response Team (CSIRT.GOV)

2.2. Postal Address

Av. Vladimir Lenine, No. 598, 7th and 8th Floors, Utomi Park Building, Maputo – Mozambique

2.3. Time Zone

Mozambique / Central Africa Time (GMT+2)

2.4. Telephone

+258 85 3053450 (Regular working hours: 07:30 – 15:30)

2.5. Fax

+258 21 428565

2.6. Email Addresses

Email for cybersecurity incident reporting:

incidente@csirt.gov.mz

Email for other CSIRT.GOV-related matters:

csirt@csirt.gov.mz

2.7. Other Communication Channels

None available.

2.8. Public Keys and Encryption Information

- **PGP Key ID:** AC24D6F6258751FD
- **PGP Fingerprint:** C480 075A 4C83 8E19 3C00 998C AC24 D6F6 2587 51FD

2.9. Team Members

Coordinator: Inalda Ernesto

Information about other team members is available upon request.

2.10. Additional Information

Further information about CSIRT.GOV can be found at:

https://www.csirt.gov.mz/

2.11. Means of Contact for Users

CSIRT.GOV can be contacted using the means listed in sections 2.2 and 2.4 to 2.7.

3. Charter

3.1. Mission

CSIRT.GOV's mission is to provide support and protection to the Mozambican Government's IT infrastructures and to promote information security awareness.

3.2. Constituency

The Government CSIRT, formally designated as **CSIRT.GOV**, serves all institutions within the Mozambican Public Administration. This includes central, local, municipal, and autonomous bodies, with a particular focus on entities operating critical services and essential infrastructures vital to the functioning of the State.

3.3. Affiliation

CSIRT.GOV is a service integrated within the **Cybersecurity Directorate of INAGE, IP**.

3.4. Authority

CSIRT.GOV is a service of **INAGE, IP**, whose governmental authority for cybersecurity is defined under **Decree No. 61/2017 of November 6**.

Under the same law, CSIRT.GOV holds technical authority to request, recommend, or execute response actions to cybersecurity incidents involving public administration institutions.

4. Policies

4.1. Incident Types and Level of Support

CSIRT.GOV responds to all types of security incidents and maintains its own incident taxonomy, available at:

https://csirt.gov.mz/wp-content/uploads/2025/07/Taxonomia-CSIRT.GOV_.pdf

The level of support provided by CSIRT.GOV varies depending on the type, severity, and scope of the ongoing incidents and the resources available for their handling.

4.2. Privacy and Data Protection Policy

CSIRT.GOV's privacy and data protection policy ensures that sensitive information may only be shared with third parties when necessary and with the express prior consent of the individual or entity concerned.

4.3. Communication and Authentication

For regular communication that does not involve confidential information, CSIRT.GOV may use conventional methods such as unencrypted email.
For secure communication, encrypted email using PGP will be employed.

Among the available communication channels, telephone and unencrypted email are considered sufficient for transmitting non-sensitive information. For sensitive information, **PGP encryption is mandatory**.

CSIRT.GOV adopts the **Traffic Light Protocol (TLP)** standard for information dissemination and sharing.

5. Services

5.1. Cybersecurity Incident Management

- **Incident Handling:** Tracking of cybersecurity incidents including detection, analysis, impact assessment, actions taken, root-cause identification, and lessons learned — ensuring efficient response and continuous security improvement.
- **Incident Coordination:** Support in crisis communication and management.

5.2. Vulnerability Management

- **Vulnerability Analysis (*Pentesting*):** Simulation of attacks to assess exploitable weaknesses and validate system security.
- **Vulnerability Alerts:** Internal and external notifications regarding critical vulnerabilities requiring immediate remediation.

5.3. Knowledge Transfer

- **Support for Establishing Institutional CSIRTs:** Assistance in creating and structuring Computer Security Incident Response Teams (CSIRTs), including defining roles, processes, and required operational tools.
- **Awareness Campaigns, Seminars, and Webinars:** Initiatives aimed at educating users and technical teams about cybersecurity best practices, emerging threats, and incident response through educational activities, lectures, and online or in-person events.

5.4. Security Event Management

- **Cybersecurity Monitoring:** Continuous process of observing and detecting threats in networks, systems, and applications using tools such as SIEM, IDS/IPS, and threat intelligence to prevent and respond to incidents.
- **Event Analysis:** Detailed analysis of logs and suspicious activities to identify patterns, anomalies, and potential security incidents, enabling proactive risk mitigation by CSIRT.GOV.

6. Disclaimer

Although every precaution is taken in preparing the information published on the website or through distribution lists, CSIRT.GOV assumes no responsibility for errors or omissions, nor for any damages resulting from the use of such information.

Incident notifications submitted to CSIRT.GOV do not replace the obligation to report to judicial authorities when the incident constitutes a criminal offense subject to complaint or private prosecution.