RFC-2350

Version: 2.0

Date:16-06-2025

Originator: Jorge Borges

1. Information about this document

This document describes the computer security incident response service of the University of Trás-os-Montes e Alto Douro , according to RFC2350. UTAD is a Portuguese University, located in the citiy of Vila Real.

1.1 Last updated

Version 2.0 published on 16-06-2025.

1.2 Distribution lists for notifications

There is no existing distribution channel for notifications of updates.

1.3 Access to this document

The updated version of this document is available at https://csirt.utad.pt

1.4 Authenticity of this document

For validation purposes, an ASCII version signed with PGP is available at https://csirt.utad.pt/wp-content/uploads/2025/06/RFC2350.txt.asc.

The PGP key used to sign is from CSIRT.UTAD and is available in section 2.8.

2. Contact information

2.1 Team name

CSIRT.UTAD– Computer Security Incident Response Team da Universidade de Trás-os-Montes e Alto Douro

2.2 Address

CSIRT.UTAD

Universidade de Trás-os-Montes e Alto Douro

Serviços de Sistemas de Informação e Comunicações

Edifício de Biblioteca Central

Quinta de Prados

5001-801 Vila Real

Portugal

2.3 Time zone

Portugal / WEST (GMT + 0,GMT + 1 in summer time)

2.4 Phone

+351 259 350 012

+351 939 899 068

2.6 Other telecommunications

Not existing.

2.7 Email addresses

csirt@utad.pt- e-mail for notification of cyber security incidents and for other matters related to CSIRT services.

2.8 Public keys and cipher information

User ID: CSIRT.UTAD (https://csirt.utad.pt) <csirt@utad.pt>

Key ID: 0x988E9C6A Key type: RSA

Key size: 4096 Expires: 2027-06-16

Fingerprint: 6005 3F8C 60D2 7515 3B4F 00D5 02E8 A07B 988E 9C6A

2.9 Team members

Coordination: Jorge Borges

Members: Fernando Rodrigues
Alberto Vasconcelos

2.10 Other information

More information about CSIRT.UTAD can be found at https://csirt.utad.pt/

2.11 User contact means

CSIRT.UTAD has the means of contact listed in sections 2.4 to 2.6.

3. Script

3.1 Mission

CSIRT UTAD's mission is to promote a culture of informatic safety in UTAD's academic community, through sensibility, counselling, collaboration, monitoring, coordination, treatment and responses to accidents of informatic safety.

3.2 Community served

CSIRT.UTAD responds to computer security incidents in the context of University of Trás os Montes e Alto Douro academic community

The ranges of IP addresses covered by its scope are:

IPV4

193.136.156.0/22

193.136.4.110/32

193.136.40.0/22

193.137.58.16/29

193.137.96.0/24

IPV6

2001:690:2240::/48

3.3 Filiation

CSIRT@UTAD is a security incident handling service integrated in the cybersecurity office of the IT Services

4. Policies

4.1 Incident types and support level

CSIRT.UTAD responds to all types of cybersecurity incidents that occur within its academic community, intrusion attempt, malicious code, availability, information collection, information security, fraud, abusive content, vulnerability, etc.

4.2 Cooperation, interaction and privacy policy

CSIRT.UTAD's privacy and data protection policy provides that sensitive information may be passed to third parties solely and exclusively in case of need and with the express prior authorization of the individual or entity to whom such information relates.

4.3 Communication and authentication

From the means of communication provided by CSIRT.UTAD, the telephone and unencrypted electronic mail are considered sufficient for the transmission of non-sensitive information. For the transmission of sensitive information the use of PGP ciphers is mandatory.

5. Services

5.1 Incident Response

CSIRT.UTAD plans to support network infrastructure administrators and systems in managing the technical and organizational aspects of security incidents. In particular, provide assistance and advice on the following aspects of incident management.

5.1.1 Incident Screening

Determine when an incident is authentic.

Evaluate and prioritize an incident.

5.1.2 Incident Coordination

Determine the organizations involved.

Contact the organizations involved to investigate the incident and take appropriate action.

Facilitate contact with other parties who can assist in resolving the incident.

Send reports to other CERTs.

Routing of information related to computer security incidents acting as a facilitator for its resolution among the various parties.

5.1.3 Incident Resolution

Advising the network and systems infrastructure administration teams on the appropriate actions to be taken.

Monitor the progress of network infrastructures and systems management teams on security issues.

Request reports.

Respond to requests.

CSIRT.UTAD collect incident statistics in the context of your institution.

5.2 Proactive activities

CSIRT.UTAD coordinates and maintains the following services to expand its capabilities:

- Advising, by the production of alerts, awareness and safety recommendations contributing to works, promotion and implementation of good information security policies and practices.

- Ensure the correct functioning and management of the digital identities lifecycle, on the access to resources and services.

- Control an infrastructure, applications and systems from the perspective of computer security vulnerabilities. Evaluating impacts, proposals for correction and / or in order to reduce the risk of data exposure, compromise of information or systems.

- Regularly do some inspections of informatic security to ensure reports, recommendations and operational continuity plans duly updated.

- Define, implement and ensure the execution of technical standards and procedures in their areas of competence.

- Actively collaborate with other units, internal or external, in their areas of competence, participation in activities, projects, etc.

6. Incident reporting forms

No forms are available for this purpose.

7. Safeguarding of liability

Although all precautions are taken in the preparation of the information disclosed in the Internet portal or through distribution lists, CSIRT.UTAD assumes no responsibility for errors or omissions, or for damages resulting from the use of this information.