RFC-2350

Versão: 2.0

Data:16-06-2025

Autor: Jorge Borges

1. Informação acerca deste documento

O presente documento descreve o serviço de resposta a incidentes de segurança informática da Universidade de Trás-os-Montes e Alto Douro (UTAD), de acordo com o RFC2350.

1.1 Data da última atualização

Versão 2.0 publicada em 2025/06/16

1.2 Listas de distribuição para notificações

Não existe um canal de distribuição para notificar alterações ao presente documento.

1.3 Acesso a este documento

A versão atualizada deste documento está disponível em https://csirt.utad.pt

1.4 Autenticidade deste documento

Para fins de validação, uma versão ASCII assinado com PGP está disponível em https://csirt.utad.pt/wp-content/uploads/2025/06/RFC2350.txt.asc.

A chave PGP utilizada para assinar é do CSIRT.UTAD e está disponível no ponto 2.8.

2. Informação de contacto

2.1 Nome da equipa

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

2.2 Morada

CSIRT.UTAD

Universidade de Trás-os-Montes e Alto Douro

Serviços de Sistemas de Informação e Comunicações

Edifício da Biblioteca Central

Quinta de Prados

5001-801 Vila Real

Portugal

2.3 Zona horária

Portugal/WEST (GMT+0, GMT+1 em horário de verão)

2.4 Telefone

+351 259 350 012 (horário normal de funcionamento - 09h00 - 18h00).

+351 939 899 068 (Contacto de emergência, fora das horas normais de funcionamento).

2.6 Outras telecomunicações

Não existentes.

2.7 Endereços de correio eletrónico

csirt@utad.pt - Correio eletrónico para notificação de incidentes de cibersegurança e outros assuntos relacionados com os serviços do CSIRT.

2.8 Chaves públicas e informação de cifra

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 Membros da equipa

Coordinação: Jorge Borges

Membros: Fernando Rodrigues
Alberto Vasconcelos

2.10 Outra informação

Mais informação sobre o CSIRT.UTAD pode ser encontrada em https://csirt.utad.pt/.

2.11 Meios de contacto para utilizadores

O CSIRT.UTAD dispõe dos meios de contacto elencados nas secções 2.4 a 2.6

3. Guião

3.1 Missão

O Csirt.Utad tem como missão promover uma cultura de segurança informática na comunidade académica da UTAD, através da sensibilização, aconselhamento, colaboração, monitorização, coordenação, tratamento e respostas a incidentes de segurança informática.

3.2 Comunidade servida

O CSIRT.UTAD responde a incidentes de segurança informática no contexto da comunidade da Universidade de Trás-os-Montes e Alto Douro.

As gamas de endereços IP abrangidos no âmbito de atuação do CSIRT.UTAD são:

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 Filiação

CSIRT.UTAD é um serviço integrado nos Serviços de Sistemas de Informação e Comunicações

4. Políticas

4.1 Tipos de incidente e nível de suporte

O Csirt.Utad responde a incidentes nas áreas de segurança informática, nomeadamente na intrusão ou tentativa de intrusão, código malicioso, disponibilidade, recolha de informação, segurança da informação, fraude, conteúdo abusivo, vulnerabilidades, etc.

Para além de incidentes de segurança informática o Csirt.Utad responde e intervém nas áreas autenticação segura, gestão do ciclo de vida de identidades digitais, cooperação, interação, definição e políticas de privacidade e proteção de dados.

4.2 Cooperação, interação e política de privacidade

A política de privacidade e proteção de dados do CSIRT.UTAD prevê que informação sensível pode ser passada a terceiros, única e exclusivamente em caso de necessidade e com a autorização prévia expressa do indivíduo ou entidade a quem essa informação diga respeito.

4.3 Comunicação e autenticação

Dos meios de comunicação disponibilizados pelo CSIRT.UTAD, o telefone e o correio eletrónico não cifrado são considerados suficientes para a transmissão de informação não sensível. Para a transmissão de informação sensível é obrigatório o uso de cifra PGP.

5. Serviços

5.1 Resposta a Incidentes

O CSIRT.UTAD prevê apoiar os administradores de sistemas na gestão dos aspetos técnica e organizacional dos incidentes. Em particular, poderemos providenciar assistência e aconselhamento com os seguimentos aspetos da gestão de incidentes.

5.1.1 Triagem de Incidentes

Determinar quando um incidente é autentico

Avaliar e priorizar um incidente

5.1.2 Coordenação de Incidentes

Determinar as organizações envolvidas

Contactar as organizações envolvidas para investigar o incidente e tomar as medidas adequadas

Facilitar o contacto com outras partes que podem ajudar na resolução do incidente

Enviar relatórios a outros CERTs

Vemo-nos como um hub de informação que conhece a instituição e consegue encaminhar os incidentes para ajudar e facilitar a resolução dos incidentes de segurança informática

5.1.3 Resolução de incidentes

Aconselhamento das esquipas locais de administração de sistemas das ações apropriadas a adotar

Acompanhar o progresso das equipas de administração de sistemas relativamente a questões de segurança

Solicitar relatórios

Dar resposta às solicitações

O CSIRT.UTAD colecionará ainda estatísticas sobre incidentes no contexto da sua constituição.

5.2 Atividades proactivas

O CSIRT.UTAD coordena e mantêm os seguintes serviços para expandir os seus recursos:

- Aconselhar, pela produção de alertas, na sensibilização e recomendações de segurança contribuindo assim para o esforço, promoção e implementação de politicas e boas práticas de segurança informática.
- Assegurar o correto funcionamento e a gestão do ciclo de vida das identidades digitais, nos acessos a recursos e serviços.
- Monitorizar a infraestrutura, aplicações e sistemas sob a perspetiva de vulnerabilidades de segurança informática. Avaliando impactos, propondo correções e/ou alterações de modo a diminuir o risco de exposição de dados, o comprometimento de informação ou sistemas.
- Efetuar regularmente auditorias de segurança informática de modo a garantir relatórios, recomendações e planos de continuidade operacional devidamente atualizados.
- Definir, implementar e garantir a execução de normas e procedimentos técnicos nas suas áreas de competência.
- Colaborar ativamente com outras unidades, internas ou externas, nas suas áreas de competência, participando em atividades, projetos ou task-forces de cariz nacional ou internacional promovendo a inovação e serviços inovadores à comunidade.

6. Formulários de report de incidentes

Não existem disponíveis formulários para o efeito.

7. Salvaguarda de responsabilidade

Embora todas as precauções sejam tomadas na preparação da informação divulgada quer no portal Internet, quer através das listas de distribuição, o CSIRT.UTAD não assume qualquer responsabilidade por erros ou omissões, ou por danos resultantes do uso dessa informação.