

# CSIRT

## Autoridade Tributária e Aduaneira

### RFC 2350

## 1. Informação acerca deste documento

Este documento descreve o serviço de coordenação da resposta a incidentes da Autoridade Tributária e Aduaneira de acordo com o RFC 2350.

### 1.1 Data da última atualização

Versão 1.0 publicada em 12 de janeiro de 2023.

### 1.2 Listas de distribuição para notificações

Não existe um canal de distribuição para notificar alterações a este documento.  
Atualizações a este documento irão estar visíveis no local indicado no ponto 1.3.

### 1.3 Acesso a este documento

A versão atualizada deste documento está disponível em  
<https://info.portaldasfinancas.gov.pt/pt/at/csirt/Paginas/default.aspx>

### 1.4 Autenticidade deste documento

Este documento está assinado com a chave PGP do nCSIRT-AT.

## 2. Informação de contacto

### 2.1 Nome da equipa

nCSIRT-AT

### 2.2 Morada:

Rua da Prata, n.º 10,  
1149-027 Lisboa

### 2.3 Zona horária

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

## 2.4 Telefone

+351 21881 2600

## 2.5 Outras telecomunicações

Não existentes.

## 2.6 Endereços de correio eletrónico

Correio eletrónico para notificação de incidentes de cibersegurança:

[ncsirt@at.gov.pt](mailto:ncsirt@at.gov.pt)

## 2.7 Chaves públicas e informação de cifra

PGP Key ID: ECC4 61FB A146 73B3

PGP Fingerprint: FOA2 8561 7B21 B844 5062 C949 0E1F 5275 6FD0 785E

A chave está disponível em:

<https://info.portaldasfinancas.gov.pt/pt/at/csirt/Paginas/default.aspx>

## 2.8 Membros da equipa

A equipa é constituída por especialistas em cibersegurança e analistas de ameaças da web.

Coordenação: José Manuel Oliveira

## 2.9 Outra informação

Mais informação sobre o nCSIRT-AT pode ser encontrada em

<https://info.portaldasfinancas.gov.pt/pt/at/csirt/Paginas/default.aspx>

## 2.10 Meios de contacto para utilizadores

O nCSIRT-AT dispõe dos seguintes meios de contacto indicados nas secções 2.4 a 2.6, sendo que é preferível o contacto por correio eletrónico.

## 3. Guião

### 3.1 Missão

Contribuir para a melhoria contínua da segurança dos sistemas de informação e da infraestrutura de TIC da Autoridade Tributária e Aduaneira, ajudando a prevenir, detetar, mitigar e dar resposta a ciberataques bem como promovendo a partilha de informação em matéria de cibersegurança.

### 3.2 Comunidade servida

O NCSIRT-AT coordena a resposta a incidentes de cibersegurança envolvendo todos os utilizadores e ativos de informação da organização.

### 3.3 Filiação

O NCSIRT-AT é um serviço integrante da Autoridade Tributária e Aduaneira. Mantém estreita coordenação com o a rede CSIRT (<http://www.redecsirt.pt/>).

### 3.4 Autoridade

O nCSIRT-AT é um núcleo constituído por despacho da Diretora-Geral da AT.

O nCSIRT-AT colabora com os diversos serviços e utilizadores da AT. Em caso de não haver resposta útil a um incidente que assim o requeira, o nCSIRT-AT poderá restringir ou bloquear o acesso, conforme estipulado nas políticas de segurança da informação.

## 4. Políticas

### 4.1 Tipos de incidente e nível de suporte

O nCSIRT-AT responde a todos os tipos de incidente de cibersegurança, nomeadamente aqueles que resultam numa violação de segurança dos seguintes tipos:

- a) Código Malicioso
- b) Disponibilidade
- c) Recolha de Informação
- d) Tentativa de Intrusão
- e) Intrusão
- f) Segurança da Informação
- g) Fraude

- h) Conteúdo Abusivo;
- i) Vulnerabilidade;
- j) Outros.

O nível de suporte dado pelo nCSIRT-AT varia consoante o tipo, gravidade e âmbito dos incidentes em curso e os recursos disponíveis para o seu tratamento.

#### 4.2 Cooperação, interação e política de privacidade

A política de privacidade e proteção de dados do nCSIRT-AT é regida pelo Regulamento Geral de Proteção de Dados (RGPD).

Dados não confidenciais poderão ser utilizados para fins estatísticos e divulgados a outros organismos.

#### 4.3 Comunicação e autenticação

Dos meios de comunicação disponibilizados pelo nCSIRT-AT, 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 necessário o uso de cifra PGP.

## 5. Serviços

### 5.1 Coordenação da resposta a incidentes

Por iniciativa própria ou sempre que solicitado para o efeito, o nCSIRT-AT, presta um serviço de coordenação de resposta a incidentes entre as entidades envolvidas e o responsável interno conforme cada caso. Esta coordenação envolve tipicamente os responsáveis diretos de uma parte da rede da AT e ISPs ou outros CSIRTs sempre que necessário. A coordenação da resposta a incidentes inclui:

- a) triagem de notificações de incidentes, bem como a análise técnica e forense;
- b) articulação com as entidades envolvidas;
- c) medidas de mitigação ou resolução e produção de recomendações;
- d) reporte de incidentes ao CNCS.

### 5.2. Atividades proactivas

- Monitorização de eventos de segurança da informação;

- Difusão de Alertas e Notificações (Internos, de Organizações Nacionais ou Internacionais);
- Análises de vulnerabilidades e auditorias de segurança (Pentests);
- ações de consciencialização para temáticas de segurança da informação e cibersegurança.

## 6. Formulário de anúncio de incidente

Não estão definidos formulários para o efeito.

## 7. Salvaguarda de responsabilidade

Embora todas as precauções sejam tomadas na preparação da informação divulgada quer no Portal Internet (<https://info.portaldasfinancas.gov.pt/pt/at/csirt/Paginas/default.aspx>). quer através das listas de distribuição, a AT não assume qualquer responsabilidade por erros ou omissões ou por danos resultantes do uso dessa informação.