

RFC 2350

Descrição do Serviço de Coordenação da Resposta a Incidentes de
Segurança Cibernética

nCSIRT.Mz — CSIRT Nacional de Moçambique

Instituto Nacional de Tecnologias de Informação e Comunicação, Instituto Público (INTIC, IP)

TLP:CLEAR

Versão 1.1

Histórico de Revisões

#	Versão	Data de Publicação
1	1.0	20/04/2023
2	1.1	13/07/2026

Elaborado com base na estrutura normativa da RFC 2350 (IETF, 1998) e nas melhores práticas internacionais de CSIRTs membros do FIRST

Índice

1. Informação acerca deste documento	4
1.1 Data da última atualização	4
1.2 Lista de distribuição para notificações	4
1.3 Locais onde este documento pode ser encontrado	4
1.4 Autenticidade deste documento	4
2. Informação de contacto	4
2.1 Nome da equipa	4
2.2 Endereço	4
2.3 Fuso horário	5
2.4 Número de telefone	5
2.5 Número de fax	5
2.6 Outros meios de comunicação	5
2.7 Endereços de e-mail	5
2.8 Chave pública e informação de cifra	5
2.9 Membros da equipa	6
2.10 Outra informação	6
2.11 Pontos de contacto para os utilizadores	6
3. Mandato	6
3.1 Missão	6
3.2 Comunidade servida (Constituency)	6
3.3 Filiação	7
3.4 Autoridade	7
4. Políticas	7
4.1 Tipos de incidentes e nível de suporte	7
4.2 Cooperação, interação e divulgação de informação	8
4.3 Comunicação e autenticação	8
5. Serviços	8
5.1 Resposta a incidentes	9
5.2 Atividades proativas	9
6. Formulário de notificação de incidentes	10
7. Salvaguarda de responsabilidade (Disclaimers)	11

1. Informação acerca deste documento

Este documento descreve o serviço de coordenação da resposta a incidentes de segurança cibernética do CSIRT Nacional de Moçambique (nCSIRT.Mz), em conformidade com a estrutura recomendada pela RFC 2350 (“Expectations for Computer Security Incident Response”, IETF, Junho de 1998) e com as boas práticas internacionalmente adotadas pelas equipas membros do FIRST (Forum of Incident Response and Security Teams).

1.1 Data da última atualização

Versão 1.1, publicada em 13/07/2026. Substitui a Versão 1.0, publicada em 20/04/2023.

1.2 Lista de distribuição para notificações

Não existe, presentemente, um canal de distribuição (mailing list) dedicado à notificação de alterações a este documento. Questões ou comentários sobre o conteúdo devem ser dirigidos a ncsirt.mz@csirt.mz.

1.3 Locais onde este documento pode ser encontrado

A versão atualizada deste documento está disponível em:

- Português e Inglês: <https://ncsirt.mz/documentos/>

Em caso de divergência entre as duas versões linguísticas, prevalece a versão em português.

1.4 Autenticidade deste documento

Este documento está assinado digitalmente com a chave PGP do nCSIRT.Mz, identificada na secção 2.8. Recomenda-se que os utilizadores verifiquem a assinatura digital antes de confiarem no conteúdo, em particular quando obtido por um canal diferente do indicado na secção 1.3.

2. Informação de contacto

2.1 Nome da equipa

nCSIRT.Mz — CSIRT Nacional de Moçambique.

2.2 Endereço

Rua José Mateus 437, R/C, Maputo, Moçambique.

2.3 Fuso horário

CAT — Central Africa Time (GMT+2). Moçambique não observa horário de verão.

2.4 Número de telefone

- (+258) 21 49 87 86/7 — contacto de emergência, fora do horário normal de funcionamento

2.5 Número de fax

- Não Aplicável

2.6 Outros meios de comunicação

- https://ncsirt.mz/formulario_ncsirt/inicio.php

2.7 Endereços de e-mail

- reportar@csirt.mz — para a notificação de incidentes de segurança cibernética;
- ncsirt.mz@csirt.mz — para outros assuntos relacionados com os serviços do nCSIRT.Mz

2.8 Chave pública e informação de cifra

A comunicação de informação sensível com o nCSIRT.Mz deve ser cifrada utilizando a seguinte chave pública PGP:

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQENBGpZ6V8BCAC31fjxbyhTC9rpnHC1AsNyirgXhlG2pSyBJZ+Kzl1Wos5+J9eh
zfrKgaUVmxlaWkmAFZh9BelNxXreY8zHom6MTkZfqDSfGqYDShFRP9Eg1DAy40UO
IO9sjWQL0Ay9107TkyqNYyUzFsnOJG9Q127o5JeA220699oyD/S0d5S/YULEjY7D
bZMUq9PY+JVj2oY9hGd5dGdXjh2HOJkiHU0eGePyooPWxHzV9EBY2RuZ6SCLyXUR
rALVZ340+74gXhXrp5H/Wyd6RtSSgSiAlY16RnLVnvlI1Q8e9A4lVi/T8zpspc5f
WaE3ilddl1g9VCh5spvEFbpEHTyX6KfSRpEpTABEBAAG0IENTSVJUIE5hY2lvmFs
IDxuY3NpcnRAY3NpcnQubXo+iQFzBBMBCABdFiEEnd7UdArAXF4syy2rPSmdlBn+
9wsFAmpZ6V8bFIAAAAAABAAObWFudTIsMi41KzEuMTIsMiwxAhsDBQkFpP/BBQsJ
CAcCAiCBhUKCQgLAgQWAgMBAh4HAheAAAJED0pnZQZ/vcL/hUIAKSvFgxgM1oT
7dCflb3lg19ebuNOXeKWK22/u22Qc36unFVPd4Mc5aVz4Gq2Hh5qvI71VZf0acsZ
5z4jpQkokzEnVazl+Ui10Q5ZkqGaa/X+IMbiMwMLCDU3errLud4bVg90v7Bk93q/
Z1QqdLs70u/XKGmPzj4ZqA0QZIUWogvgTov3Ajpt6f5ZSHOJYtvCgNbYxliseQfU
yxRBfZrZEoUStlIdizA2cs7mxMwWVFOvwgDszmTawKSAh05EuToC5TF7razuf9J
TfKXRMPG9XJZh7bozCMYvzGtZw1z9S8IqU30tdftQK9Ws+EN0s9B08Diy8BYcE4x
BJwv62EtwGy5AQ0EalnpXwEIAL1UO+3S5OSkYPPQPqttvhviffpIEybQeGNCIlsX
EDdNas1AAmZV56oWROuTHmlXgYFTa8M8IjpHtXfnmOb2orQgBSgej3ZZhuvH3mbx
OGdflOczh4BwnO/nFL8bP3zVCBmOjSuhF4pkxd9LBSc/rX9sh78PejxAGx+xINW6
IO3yjFibGLhKdZ3oc++qM/8dPxOths3GwQl8OCw7BFfc9OPqYrKColxpSCs5SIx
/cs0KYWKtLnLHHLjSlkCLNgQ6gAUJ7ZO45pX4QLR+Waz4v8QZBYSMN+x4KMmeZE7
HKNYA02mTAEtl+Y3W7yNpFTctVQchknuBgv6/omMLEvzEFUAEQEAAkBWAAQYAQgA
```

```
QhYhBJ3e1HQKwFxeLMstqz0pnZQZ/vcLBQJqWelfGxSAAAAAAQADm1hbnUyLDlu
NSsxLjEyLDIsMQIbDAUJBaT/wQAKCRA9KZ2UGf73C1VoB/9Ev5pBJlgeCEHmUSRf
L8+FOkFPORsmGSBfp6I7lJDR7uPe8oFSWsSzAMkT/wjadUM1dL2w2FmCO6BgN6C
ptLRVajbC7f6/b+3cNIO554j4H1qM/9q+Fy8juUXrubUJQLIVBwT2XHyHUYiwVAb
lCqj4ktzoS34//4eUFVUiTQ6aXzyVKMWbVMbRCLJyzYTdRMeNEiPxPnst5JWfyz2
2ugtGgU2jFPwPZp7UNl5xYpgpkBwJCpF38SyaxRO0kMTq09nyQSJZPhSvvJGqHfg
KpFPnUkQeOENIPEOMdMa7f/JELFzIDRVeDBAr5XTDfbZuDluZPb7wSqbuwJjGelM
9UTt
=gfg6
-----END PGP PUBLIC KEY BLOCK-----
```

A chave está também disponível para download em <https://ncsirt.mz>.

2.9 Membros da equipa

Coordenação: Sérgio Guivala.

A informação sobre os restantes membros da equipa está disponível apenas mediante solicitação, por motivos de segurança operacional.

2.10 Outra informação

Informação adicional sobre o nCSIRT.Mz pode ser consultada em <https://ncsirt.mz>.

2.11 Pontos de contacto para os utilizadores

O ponto de contacto preferencial do nCSIRT.Mz é o indicado na secção 2.7 (e-mail), complementado pelos meios de contacto telefónico e postal referidos nas secções 2.2 e 2.4. O horário normal de atendimento é das 7h30 às 15h30 (CAT).

3. Mandato

3.1 Missão

Criar e desenvolver uma capacidade nacional de resposta a incidentes cibernéticos que garanta um ambiente seguro no ciberespaço moçambicano, em particular, e no ciberespaço mundial, em geral.

3.2 Comunidade servida (Constituency)

De forma geral, a comunidade servida abrange o ciberespaço de interesse nacional, incluindo qualquer dispositivo pertencente a uma rede ou bloco de endereçamento atribuído a um operador de comunicações eletrónicas, instituição, pessoa coletiva ou singular com sede em território moçambicano, ou fisicamente localizado em território moçambicano.

3.3 Filiação

O nCSIRT.Mz é um serviço integrante do Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), entidade reguladora de TIC sob tutela do Ministério das Comunicações e Transformação Digital (MCTD).

3.4 Autoridade

A Lei n.º 3/2017, de 9 de Janeiro (Lei das Transações Eletrónicas), designa o INTIC como entidade reguladora de Tecnologias de Informação e Comunicação (TIC) no país. Nos termos do Decreto n.º 90/2020, de 9 de Outubro, compete ao INTIC estabelecer mecanismos que garantam a segurança e a integridade dos sistemas e operações informáticas, bem como propor um quadro legal de proteção de dados pessoais e de combate a crimes cibernéticos.

A Política Nacional de Segurança Cibernética e a respetiva estratégia de implementação, aprovadas pelo Conselho de Ministros em Dezembro de 2021 através da Resolução n.º 69/2021, designam o INTIC como entidade responsável pelo estabelecimento da equipa Nacional de Resposta a Incidentes Cibernéticos de Moçambique (nCSIRT.Mz).

O Presidente do Conselho de Administração do INTIC, no uso das competências conferidas pela alínea c) do artigo 6.º do Decreto n.º 90/2020, de 9 de Outubro (Estatuto Orgânico do INTIC), determinou o estabelecimento do nCSIRT.Mz através do Despacho n.º 6/PCA/INTIC,IP/001.1/2022.

4. Políticas

4.1 Tipos de incidentes e nível de suporte

O nCSIRT.Mz responde a todos os tipos de incidentes de segurança cibernética, nomeadamente os que resultam numa violação de segurança das seguintes categorias:

- Código malicioso
- Disponibilidade
- Recolha de informação
- Tentativa de intrusão
- Intrusão
- Segurança da informação
- Fraude
- Conteúdo abusivo
- Vulnerabilidade

O nível de suporte prestado varia consoante o tipo, a gravidade e o âmbito dos incidentes em curso, bem como os recursos disponíveis para o seu tratamento. Em condições normais de funcionamento, é objetivo do nCSIRT.Mz assegurar uma primeira resposta no prazo de um dia útil.

O nível de suporte varia também em função da natureza da entidade afetada: são assegurados todos os serviços descritos na secção 5 às entidades do Estado, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais. Às restantes entidades e indivíduos da comunidade servida são assegurados os serviços de coordenação da resposta a incidentes e de alertas de segurança.

Em caso de aumento considerável da severidade e do âmbito dos incidentes, ou de incidente de larga escala, é dada prioridade ao tratamento de incidentes que afetem entidades do Estado, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais.

4.2 Cooperação, interação e divulgação de informação

A política de privacidade e proteção de dados do nCSIRT.Mz prevê que informação sensível apenas pode ser partilhada com terceiros em caso de necessidade e mediante autorização prévia e expressa do indivíduo ou entidade a quem essa informação diga respeito.

O nCSIRT.Mz coopera, sempre que necessário, com outras equipas de resposta a incidentes nacionais e internacionais, autoridades competentes e prestadores de serviços, no estrito respeito pelos princípios de confidencialidade acima referidos.

4.3 Comunicação e autenticação

Dos meios de comunicação disponibilizados pelo nCSIRT.Mz, o telefone e o e-mail 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, com recurso à chave pública indicada na secção 2.8.

O nCSIRT.Mz adota o padrão TLP (Traffic Light Protocol), na sua versão mais recente definida pelo FIRST, para a disseminação e partilha de informação. Toda a informação partilhada deve ser rotulada de forma explícita com a classificação TLP aplicável.

5. Serviços

Os serviços do nCSIRT.Mz estão organizados em torno de duas grandes áreas: a resposta a incidentes e as atividades proativas de prevenção e capacitação, em linha com a estrutura habitualmente adotada por equipas membros do FIRST.

5.1 Resposta a incidentes

Serviço disponibilizado a toda a comunidade servida.

5.1.1 Triagem de incidentes

Recepção, registo e análise preliminar das notificações de incidentes, incluindo a sua avaliação técnica e forense inicial, com vista à determinação da prioridade e do encaminhamento adequado.

5.1.2 Coordenação da resposta a incidentes

Sempre que solicitado, o INTIC, através do nCSIRT.Mz, presta um serviço de coordenação da resposta a incidentes entre as entidades envolvidas. Esta coordenação envolve tipicamente as vítimas dos ataques e os provedores de serviços de Internet (ISP) ou outros CSIRT, sempre que necessário, e inclui:

- 1) Triagem de notificações de incidentes e respetiva análise técnica e forense;
- 2) Articulação com as entidades nacionais e internacionais envolvidas;
- 3) Produção de recomendações de mitigação e/ou de resolução do incidente.

A coordenação da resposta a incidentes pode partir da iniciativa do nCSIRT.Mz — por exemplo, numa situação de incidente de larga escala — ou ser solicitada através dos canais designados para o efeito.

5.1.3 Suporte on-site

Disponibilizado a entidades do Estado, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais.

O suporte on-site prevê o apoio, nas instalações do requerente, de técnicos especializados do nCSIRT.Mz, para análise e resposta a incidentes de segurança cibernética, podendo incluir:

- 1) Análise forense a máquinas ou hardware;
- 2) Análise de tráfego;
- 3) Análise de malware;
- 4) Articulação com outros CSIRT nacionais ou internacionais;
- 5) Produção de recomendações;
- 6) Apoio na aplicação de medidas de mitigação e resolução.

O nCSIRT.Mz não executa as medidas de mitigação ou de resolução acima referidas; essa responsabilidade é de cada uma das entidades intervenientes.

5.2 Atividades proativas

5.2.1 Alertas de segurança

Disponibilizado a toda a comunidade servida. Consiste em alertar as partes interessadas, incluindo o público em geral, para novos riscos de segurança cibernética, disponibilizando a informação necessária à sua proteção e/ou remediação. Para o efeito, o INTIC desenvolve duas atividades:

- 1) Em articulação com as restantes autoridades nacionais, emissão de um código único de perigosidade nacional;
- 2) Produção e disseminação, às partes interessadas, de alertas de segurança.

5.2.2 Capacitação de CSIRT

Disponibilizado a entidades do Estado, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais. Tem por objetivo melhorar a capacidade nacional de resposta a incidentes de segurança cibernética, através da criação de novos CSIRT e do reforço das capacidades dos já existentes, designadamente através de:

- 1) Ações de formação para técnicos e decisores que operem, ou pretendam vir a operar, um CSIRT;
- 2) Coordenação de exercícios nacionais e promoção da participação em exercícios internacionais de segurança cibernética;
- 3) Definição de um conjunto mínimo de capacidades técnicas, operacionais e humanas para um CSIRT;
- 4) Divulgação de boas práticas para a gestão de incidentes de segurança cibernética;
- 5) Consultoria para a criação de novos CSIRT.

6. Formulário de notificação de incidentes

As notificações de incidentes devem ser submetidas ao formulário disponível em https://ncsirt.mz/formulario_ncsirt/inicio.php, devendo incluir, sempre que possível, os seguintes elementos:

- Identificação e dados de contacto do notificador;
- Data e hora (com fuso horário) em que o incidente foi observado;
- Descrição do incidente e sistemas, redes ou serviços afetados;
- Endereços IP, domínios, URL ou outros indicadores de compromisso relevantes;
- Evidências disponíveis (registos, capturas de ecrã, amostras);
- Medidas já adotadas, se aplicável.

7. Salvaguarda de responsabilidade (Disclaimers)

Embora sejam tomadas todas as precauções na preparação da informação divulgada, quer na página, quer através das listas de distribuição e outros meios, o nCSIRT.Mz não assume qualquer responsabilidade por erros ou omissões, ou por danos resultantes do uso dessa informação.

A notificação de incidentes ao nCSIRT.Mz não substitui a comunicação à autoridade judiciária ou ao órgão de polícia criminal competente, quando os incidentes configurem também um ilícito criminal cujo procedimento penal dependa de queixa ou de acusação particular.

Este documento não constitui um contrato e está sujeito a revisão periódica. A versão em vigor é sempre a publicada nos locais indicados na secção 1.3.