RFC 2350

1. Informação acerca deste documento

Este documento descreve o serviço de coordenação da resposta a incidentes de cibersegurança do CSIRT Nacional de Moçambique (nCSIRT.Mz) de acordo com o RFC 2350.

1.1 Data da última atualização

Versão 1.0 publicada em 20/04/2023.

1.2 Listas de distribuição para notificações

Não existe um canal de distribuição para notificar alterações a este documento.

1.3 Acesso a este documento

A versão atualizada deste documento está disponível em https://ncsirt.mz/rfc-2350

A versão em língua inglesa está disponível em https://ncsirt.mz/rfc-2350_Eng/

1.4 Autenticidade deste documento

Este documento está assinado com a chave PGP.

2.Informação de contacto

2.1 Nome da equipa

nCSIRT.Mz

2.2 Endereço postal

Rua Jose Mateus 437 R/C

Maputo

Mocambique

2.3 Zona horária

ACT (GMT +2)

2.4 Telefone

+258800 909 909 (09h00 - 18h00) – Ainda não operacional

+258 843649222 (Contacto de emergência, fora das horas normais de funcionamento)

2.5 Outras formas de comunicação

e-mail:reportar@csirt.mz

2.7 Endereços de correio electrónico

Correio electrónico para notificação de incidentes de cibersegurança:

reportar@csirt.mz

Correio electrónico para outros assuntos relacionados com os serviços nCSIRT.Mz:

ncsirt@csirt.mz

2.8 Chave pública e informação de cifra

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

mQGNBGU2OVkBDADFvbAHn1oF5on8kYUrN1fLUMvP7Mlnh0Oexwm3eiv+g3tGK7GK
3s4KFqjNkCY0p1EVHvOvs7Xyh8kRRiGwLo0F9povLVDwJ5JdZxB918TtxZzvR+oI
dVihsuDQifZI1J5gfqMrpbYy6U6ELT0SfF02zeypI5QQ3MxAbNCaFJt/Vcv2eSaH
9eLmg/m3EOuRLCja/qrTcvHAFypsC0UYqm5cGMLUuV4EgY0qKp7XOH35B/UGXDS0
METrM30HMAQTAbmr94n1u5RawtD/2T7369crpOnDWz7dTcFLkX2/53IZRd7OE3bg
ukm/zdtdXZ9gTJ50TaJxj9FlbEwHA4brdebiIPVTAk0uaKxkfT9KPpLBNnPerO3C
eS/fkSKN4v7zAHS9dR0E2Ry01PpKjp9ayxzP1bYfPfxh0MrmAxVrklPaEXYFGUaC
vsUZ4CqZpvrf6HnK5/4O2zq2eRZ2ppANgL29K77u9ilcwBTsUt3cqGnymYy/SCbt
FRXVqjpIEG9VNPMAEQEAAbQYbmNzaXJ0IDxuY3NpcnRAY3NpcnQubXo+iQHXBBMB
CABBFiEEzHc5Y/TyHNUSMLqN7SEUOW1rVwYFAmU2OVkCGyMFCQPDw0cFCwkIBwIC
IgIGFQoJCAsCBBYCAwECHgcCF4AACgkQ7SEUOW1rVwbazAwAvVSPoFuq9sNHsqgV
78ZAd198JLgV03mkb0Foz5AEvrJej9mhJSrdpNfZbt6NmqMwsNlD9E7S1EROaJZw
mxP1pAfrGM7CjyTWvUZmudz6vku+KrnfKW5r8jYwEmYFg8Chp1kTie4301x9Ie9R
9fV/OoT2dC+jcwExUfavkL+8TBu2v5DQdMR5z96uvwOy+/1qZDea7FZTKZdqgmON
0LidrE+UUBWD5q0W3u6+VWhDNFZeAFpJqTwNJkJHTnrn7wf+5g8jiMhSiXlgVP7M

zyxBUt25RDALa+6SITL/mYoq6dKeU0lx8FuZQ/firHLW4k76oYseVXAMGsKcRyMQ
9fDU3levR59DrmNTxXtxuf7c/WPrH58DSpdTaeGu4CEOf3otXo0qT9h5a/nR3Oo7
Szl5IAw6wV/NrJCVhv0jEiHjyIL5/EJNn9NpW/MBLdwQuRzyKUSlof8LOoGKVt3X
JON95b43CTu+RBAecu88utmv3PTH01tqReQiYtesHFwX3AwduQGNBGU2OVkBDAC/
CujkgD8xk+3/qwlwjTDSYGItbMffyS1FwxRvZtrSRgtRgIqPA8zQsxdlqhe9jUF/
UsN1f2EZE+zmwVVrutjyybAN0EsstYRQgpTPz4EYoszolq65Wp8Rhnj3ma0RM7Dx
oBheSH6lXL02CqO1eXlVbE0LnlBOKp8xC5wsIhur8GyGr9DItyCh6JzQnHyB4vCp
NNeCklQgCMScNQB+FsG/hMUshLDiMfRjSgt+XL88zeXz5SIbuPMcr4UtDvzRIo0n
gvDyq92bIiSXT2wN7RrJPQqNhGOC4FW6529sabEyDObAsfHs1yE5B+9mcs1UrP5G
mc9ddzyiKZE8G6iAAfEoTVXqa5cS0Fa4EJP+uAmIjyRpMJ8Du8iuCHjg3uJ7DrVU
FXNMVGh17kPckHQChkIToPzLttAr6aIGSwHgPPcx0mLAdmc/ug8H0YLVcbRSyaX8
oY3r3xGK9UkESHn7oAVpJ+M2a9vCdOpVpi2e1PXXIkSytrqfAesX+AMuhWBhVIcA
EQEAAYkBvAQYAQgAJhYhBMx3OWP08hzVEjC6je0hFDlta1cGBQJlNjlZAhsMBQkD
w8NHAAoJEO0hFDlta1cGOAcL/3u/2zDh/+eqyxSUsLK7xTCdINV2LCsg0at+0XAE
lTHRh9JLrIrXTHIKiCL1FbP9WwbTzliwLVBAs7k+dfvwySy78AcGM0z8VrJ32Qyo
6QV87H5/mDnjl9RHacLAB4+CXDh0lfl+IPPJjhQyo7aibPUiAOdF4c2b0kANr9XD
EpU14hpqI7w6n4/KuxrwKX4eRYwtHF+DNx2SKmZuaqMM1lnXTybwchJltaCPgOUB
8OoFEnbw9INhjAY5ERiPAoWJsd9F63ql/lteBxpRTyr36HZnFDvPNH72kk5WKX+9
XRIXUOfWawOKasCkJo34b6D6xsLWL4n50qQkJkdRsUdJJPeIjqdwLNfn8GO5bJO4
84+cPzAfsFcikN3QyVL9jcIPh4ogOI+BHB3OJwtl55hkST3iDwdqbksPvaXMRqas
7qf2O3K/s406/TQyKYZL4PGQHp0ycSTWBePty2Tqi1FPbBusBf1KTFFijbq6RUCu
PGhSlxJykBdZGGJi89dfXY93+A==
=pbgS

-----END PGP PUBLIC KEY BLOCK-----

A chave está disponível em: https://ncsirt.mz

2.9 Membros da equipa

Coordenação: Sérgio Guivala

A informação sobre os restantes membros da equipa apenas está disponível por solicitação.

2.10 Outra informação

Mais informação sobre o nCSIRT.Mz pode ser encontrada em https://csirt.mz.

2.11 Meios de contacto para utilizadores

O MZ_nCSIRT dispõe dos meios de contacto elencados nas secções 2.2 e 2.4 a 2.7.

3. Guião

3.1 Missão

Criar e desenvolver uma capacidade nacional de resposta a incidentes cibernéticos que garanta um ambiente seguro no espaço cibernético Moçambicano em particular e no Ciberespaço Mundial em geral.

3.2 Comunidade servida

De uma forma geral, o ciberespaço de interesse nacional, incluindo qualquer dispositivo Pertencente a uma rede ou bloco de endereçamento atribuído a um operador de Comunicações electrónicas, instituição, pessoa coletiva ou singular com sede em território Moçambicano, ou que esteja 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 TICs sob Tutela do Ministério de Ciência Tecnologia e Ensino Superior (MCTES).

3.4 Autoridade

Lei 3/2017 de 9 de Janeiro – Lei das Transações Eletrónicas (LTE), indica o INTIC como Entidade Reguladora de Tecnologias de Informação e Comunicação (TIC) no pais. De acordo com o decreto n°90/2020 de 9 de Outubro, compete ao INTIC a responsabilidade de estabelecer mecanismos para garantir a segurança e integridade dos sistemas e operações informáticas, bem como propor um quadro legal de proteção de dados pessoais e de combatea crimes cibernéticos.

A Politica Nacional de Segurança Cibernética e sua estratégia de Implementação aprovada pelo conselho de Ministros em Dezembro 2021 através d a resolução 69/2021 indica o INTIC como entidade responsável para estabelecer a equipe Nacional de Resposta a Incidentes Cibernéticos em Moçambique (nCSIRT.Mz).

O presidente do conselho de Administração do INTIC, no âmbito das competências que lhe são conferidas ao abrigo do disposto da alínea c), do artigo 6 do Decreto n.º 90/2020, de 9 de Outubro, Estatuto Orgânico do Instituto Nacional de Tecnologias de Informação e Comunicação, determino determinou o Estabelecimento do nCSIRT.mz através do despacho nº 6/PCA/INTIC,IP/001.1/2022:

4. Políticas

4.1 Tipos de incidente e nível de suporte

O nCSIRT.Mz 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) Vulnerável

O nível de suporte dado pelo nCSIRT.Mz varia consoante o tipo, gravidade e âmbito dos incidentes em curso e os recursos disponíveis para o seu tratamento. Em condições de funcionamento normais é um objetivo do nCSIRT.Mz dar uma primeira resposta no espaço de um dia útil.

O nível de suporte prestado pelo nCSIRT.Mz em condições normais varia também em função da entidade da comunidade servida afetada, sendo assegurados todos os serviços referidos em (5.) a entidades do Estado, operadores de Infraestruturas Críticas, operadores de serviços essenciais e prestadores de serviços digitais. Às restantes entidades e indivíduos constantes da Comunidade servida são assegurados os serviços de Coordenação da resposta a incidentes e Alertas de Segurança.

Em caso de um aumento considerável da severidade e âmbito dos incidentes ou de incidente de larga-escala, será dada prioridade ao tratamento de incidentes das entidades do Estado, operadores de Infraestruturas Críticas, operadores de serviços essenciais e prestadores de serviços digitais.

4.2 Cooperação, interação e política de privacidade

A política de privacidade e proteção de dados do nCSIRT.Mz 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 nCSIRT.Mz, 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.

O nCSIRT.Mz adota o standard TLP (Traffic Light Protocol) para a disseminação e partilha de informação.

5. Serviços

5.1 Coordenação da resposta a incidentes

A toda a Comunidade servida.

Sempre que solicitado para o efeito, o INTIC, através dos serviço nCSIRT.Mz, presta um serviço de coordenação de resposta a incidentes entre as entidades envolvidas. Esta coordenação envolve, tipicamente as vítimas dos ataques e ISPs ou outros CSIRTs sempre que necessário. A coordenação da resposta a incidentes inclui:

1) triagem de notificações de incidentes, a sua 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-lhe solicitada pelos canais designados para o efeito.

5.2 Suporte On-Site

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 cibersegurança. Dependendo das necessidades em concreto, este apoio pode, entre outros, 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 atrás referidas. Esta responsabilidade é de cada uma das entidades intervenientes.

5.3 Capacitação CSIRTs

A entidades do Estado, operadores de Infraestruturas Críticas, operadores de serviços essenciais e prestadores de serviços digitais.

Melhorar a capacidade nacional de resposta a incidentes de cibersegurança através da criação de novos CSIRTs e do desenvolvimento das capacidades dos já existentes. Para esse efeito, o INTIC e o nCSIRT.Mz promovem ou desenvolvem um conjunto de actividades com vista à capacitação de CSIRTs em território nacional, designadamente:

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 portuguesa em exercícios de cibersegurança internacionais;
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 cibersegurança;
5) Consultoria para a criação de novos CSIRT.

5.4 Alertas de Segurança

A toda a Comunidade servida.

Alertar as partes interessadas, incluindo o público em geral, para novos riscos de cibersegurança,

prestando, igualmente, a informação necessária para a sua proteção e/ou remediação. Assim, o INTIC desenvolve duas actividades:

1) Em articulação com as restantes autoridades nacionais, emite um código único de perigosidade nacional;

2) Produz e dissemina às partes interessadas, alertas de segurança

6. 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 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 se substitui à comunicação à autoridade judiciária ou ao órgão de polícia criminal competente, quando esses incidentes configurem também um ilícito criminal cujo procedimento penal dependa de queixa ou de acusação particular.