INAGE,IP

Instituto Nacional de Governo Electrónico, Instituto Público

DIVISÃO DE SEGURANÇA CIBERNÉTICA

Equipa de Resposta a Incidentes de Segurança Cibernética do Governo

CSIRT.GOV

RFC 2350

Maputo, Julho de 2025

1. Informação acerca deste documento

Este documento descreve o serviço de resposta a incidentes de cibersegurança do Equipa de Resposta a Incidentes de Segurança Cibernética do Governo (CSIRT.GOV) de acordo com o RFC 2350.

1.1. Data da última actualização

Versão 1.1 publicada em 2025/07/14

Segunda-feira, 14 de Julho, 12:59:15 (GMT +2)

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 actualizada deste documento, em português, pode ser encontrada em: https://csirt.gov.mz/documentos/rfc-2350-csirt-pt.pdf
A versão actualizada deste documento, em inglês, pode ser encontrada em: https://csirt.gov.mz/documentos/rfc-2350-csirt-en.pdf

1.4. Autenticidade deste documento

Este documento está assinado com a chave PGP do CSIRT.GOV.

2. Informação de contacto

2.1. Nome da equipa

Equipa de Resposta a Incidentes de Segurança Cibernética do Governo (CSIRT.GOV)

2.2. Endereço postal

Av. Vladimir Lenine, Nº 598, 7º e 8º Andares, Predio Utomi Park, Maputo-Moçambique

2.3. Zona horária

Moçambique/Central Africa Time (GMT+2)

2.4. Telefone

+258 82 3053450 (Horário normal de funcionamento 07:30 – 15:30)

2.5. Fax

+258 21 428565

2.6. Endereço de correio electrónico

Correio electrónico para notificação de incidentes de cibersegurança: incidente@csirt.gov.mz
Correio electrónico para outros assuntos relacionados com os serviços CSIRT.GOV: csirt@csirt.gov.mz

2.7. Outras telecomunicações

Não existentes.

2.8. Chaves públicas e informação de cifra

PGP key ID: AC24D6F6258751FD
PGP Fingerprint: C480 075A 4C83 8E19 3C00 998C AC24 D6F6 2587 51FD

2.9. Membros da equipa

Coordenação: Inalda Ernesto
A informação sobre os restantes membros da equipa apenas está disponível por solicitação.

2.10. Outra Informação

Mais informação sobre o CSIRT.GOV pode ser encontrada em https://www.csirt.gov.mz/.

2.11. Meios de contacto para utilizadores

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

3. Guião

3.1. Missão

O CSIRT.GOV tem como missão prestar apoio e proteção a infraestruturas de TI do Governo de Moçambique e promover a conscientização sobre segurança da informação.

3.2. Comunidade servida

O CSIRT do Governo designado formalmente como CSIRT.GOV – presta serviços a todas as instituições da Administração Pública Moçambicana. Este apoio inclui instituições centrais, locais, autárquicas e organismos autónomos, com foco especial nas entidades que operam serviços críticos e infraestruturas essenciais para o funcionamento do Estado.

3.3. Filiação

O CSIRT.GOV é um serviço integrante da Direcção de Segurança Cibernética do INAGE, IP.

3.4. Autoridade

CSIRT.GOV é um serviço do INAGE, IP cuja competência de autoridade governamental para a cibersegurança se encontra definida no Decreto de criação do INAGE, IP n.°61/2017 de 6 de Novembro.

Nos termos da mesma lei o CSIRT.GOV tem autoridade técnica para solicitar, recomendar ou executar acções de resposta perante incidentes cibernéticos que envolvam instituições da Administração publica.

4. Políticas

4.1. Tipos de Incidente e nível de suporte

O CSIRT.GOV responde a todos os tipos de incidente de segurança e possui sua própria taxonomia, disponível em https://www.csirt.gov.mz/documentos/taxonomia.pdf

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

4.2. Tipos de incidente e nível de suporte

A política de privacidade e protecção de dados do CSIRT.GOV 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

Para uma comunicação normal que não contém/envolve informações confidenciais, o CSIRT.GOV pode usar métodos convencionais, como email não

criptografado. Para comunicação segura, será utilizado o email criptografado por PGP.

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

O CSIRT.GOV adopta o standard TLP (*Traffic Light Protocol*) para a disseminação e partilha de informação.

5. Serviços

5.1. Gestão de Incidentes de Segurança Cibernética

- **Registo de Incidentes –** documentação e rastreio de incidentes de segurança cibernética, incluindo detecção, análise, impacto, acções tomadas e lições aprendidas, garantindo resposta eficiente e melhoria contínua da segurança.
- **Análise de Incidentes -** Identificação da causa de um ataque e mitigação dos seus efeitos;
- **Análise forense digital** – Investigação de incidentes para determinar origem e impacto;
- **Mitigação e Recuperação** – Implementação de medidas para restaurar sistemas e prevenir novos ataques;
- **Coordenação de tratamento de incidentes** – Apoio na comunicação e gestão de crises;

5.2. Gestão de Vulnerabilidades

- **Pesquisa de Vulnerabilidades-** Identificação de falhas de segurança em sistemas, redes e aplicações por meio de fontes públicas e ferramentas especializadas;
- **Relatórios de Vulnerabilidades -** Documentação das vulnerabilidades descobertas, incluindo detalhes técnicos, criticidade (CVSS) e recomendações de correção;

- **Análise de Vulnerabilidades (*Pentest*) -** Simulação de ataques para avaliar a exploração de falhas e validar a segurança dos sistemas;
- **Coordenação de Vulnerabilidades -** Organização e priorização das vulnerabilidades descobertas, garantindo comunicação e mitigação eficaz;
- **Envio de Alertas Sobre Vulnerabilidades -** Notificação interna e externa sobre falhas críticas para ações imediatas de correção;
- **Correção de Vulnerabilidades -** Aplicação de *patches*, ajustes de configuração e outras medidas para eliminar ou mitigar riscos de segurança.

5.3. Sensibilização

- **Colecta de Informação –** Obtenção de dados de ameaças, incidentes e vulnerabilidades, utilizando fontes internas (logs, *SIEM*, *IDS/IPS*) e externas (inteligência de ameaças, feeds de CVE, fóruns de segurança)
- **Campanhas de Sensibilização, seminários e webinares -** iniciativas para informar e formar utilizadores e equipas técnicas sobre boas práticas de cibersegurança, ameaças emergentes e resposta a incidentes, através de ações educativas, palestras e eventos online ou presenciais.

5.4. Transferência de Conhecimento

- **Apoio no Estabelecimento de CSRIT's Institucionais -** Assistência na criação e estruturação de Equipas de Resposta a Incidentes de Segurança Informática (CSIRTs), incluindo definição de funções, processos e ferramentas necessárias para operar eficazmente.
- **Exercícios de Segurança Cibernética -** Simulações de ataques e incidentes para testar a capacidade de resposta das equipas de segurança, melhorar processos e reforçar a resiliência cibernética das instituições.
- **Assessoria na Elaboração de Política e Procedimentos de Segurança -** Apoio técnico na definição de normas e boas práticas de cibersegurança, garantindo conformidade com regulamentos e melhorando a proteção da informação.

5.5. Gestão de Eventos de Segurança

- **Monitoramento da Segurança Cibernética -** Processo contínuo de observação e deteção de ameaças em redes, sistemas e aplicações, utilizando ferramentas como *SIEM, IDS/IPS* e *threat intelligence* para prevenir e responder a incidentes;

- **Análise de Eventos –** análise detalhada de *logs* e actividades suspeitas para identificar padrões, anomalias e possíveis incidentes de segurança, permitindo que o CSIRT actue de forma proativa na mitigação de riscos

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 CSIRT.GOV não assume qualquer responsabilidade por erros ou omissões, ou por danos resultantes do uso dessa informação.

A notificação de incidentes ao CSIRT.GOV não se substitui à comunicação à autoridade judiciária, quando esses incidentes configurem também um ilícito criminal cujo procedimento penal dependa de queixa ou de acusação particular.