



ECOWAS COMMISSION  
COMMISSION DE LA CEDEAO  
COMISSÃO DA CEDEAO

## NONAGÉSIMA TERCEIRA SESSÃO ORDINÁRIA DO CONSELHO DE MINISTROS

Abuja, 13 de dezembro de 2024

### **DIRETIVA C/DIR. 2/12/24 RELATIVA À MEDIDAS DE REFORÇO DA CONFIANÇA NO CIBER/TIC (MRC)**

#### **O CONSELHO DE MINISTROS,**

**CIENTE** dos Artigos 10, 11 e 12 do Tratado da CEDEAO revisto conforme alterado que institui o Conselho de Ministros e define a sua composição e competências;

**CIENTE** dos Artigos 27, 32 e 33 do Tratado da CEDEAO, revisto sobre ciência e tecnologia, comunicação e telecomunicações;

**CIENTE** do Ato Adicional A/SA.1/01/07 da CEDEAO relativo à harmonização das políticas e do quadro regulamentar do Setor das Tecnologias da Informação e Comunicação (TIC);

**CIENTE** do Ato Adicional A/SA.1/01/10 da CEDEAO sobre a proteção de dados pessoais na CEDEAO;

**CIENTE** do Ato Adicional A/SA.2/01/10 da CEDEAO sobre transações eletrónicas na CEDEAO;

**CIENTE** da Diretiva C/DIR.1/08/11 relativa à luta contra a cibercriminalidade na CEDEAO;

**CIENTE** da Diretiva C/DIR.1/01/21 relativa à adoção da Estratégia Regional de Cibersegurança e Cibercriminalidade;

**CIENTE** da Diretiva C/DIR.2/01/21 que adota a Política Regional de Proteção das Infraestruturas Essenciais da CEDEAO;

**CONSIDERANDO** o rápido avanço das tecnologias da informação e da comunicação (TIC), que transformou o ciberespaço num ambiente complexo e expôs as nações a ameaças cibernéticas significativas, tanto por parte de intervenientes estatais como não estatais;

**CONSIDERANDO IGUALMENTE** que estas ameaças são cada vez mais frequentes e têm impactos transnacionais, incluindo o potencial para perturbar as infraestruturas essenciais e disseminar a desinformação;

**CONSCIENTE** que as Medidas de Reforço da Confiança (MRC) constituem instrumentos essenciais para promover a ciberestabilidade internacional, reforçando a ciber-resiliência através da cooperação internacional e da coordenação interagências;

**RECONHECENDO** a necessidade de transparência, cooperação, confiança e reforço das capacidades entre os Estados-membros da CEDEAO no ciberespaço para garantir a estabilidade e o crescimento na região;

**TENDO PRESENTE** os relatórios do Grupo de Peritos Governamentais das Nações Unidas sobre a Evolução no Domínio da Informação e das Telecomunicações no Contexto da Segurança Internacional, do Grupo de Trabalho Aberto sobre a evolução no domínio da informação e das telecomunicações no contexto da segurança internacional e do Grupo de Trabalho Aberto sobre a segurança e a utilização das tecnologias da informação e da comunicação;

**CONSTATANDO** que a operacionalização e o reforço eficazes das MRC são contribuições vitais e fundamentais para um ambiente de TIC aberto, seguro, estável e pacífico;

**CONSIDERANDO** a necessidade de aumentar a transparência e a cooperação dos Estados-membros e de reduzir a utilização maliciosa das Tecnologias de Informação e Comunicação (TIC);

**DESEJOSO** de adotar Medidas de Reforço da Confiança (MRC) para orientar o comportamento dos Estados-membros e promover a estabilidade no cenário cibernético global;

**SOB RECOMENDAÇÃO** da 19ª Reunião de Ministros responsáveis pelas Telecomunicações, TICs e Economia Digital, realizada em Cotonou, de 2 a 4 de outubro de 2024;

**APÓS O PARECER** do Parlamento através da sua Mesa reunida com carácter de urgência em Abuja, de 6 a 14 de dezembro de 2024, nos termos do n. 3 alínea b) (vii) do artigo 25 do Ato Complementar A/SA.1/12/16 relativo ao Reforço das Prerrogativas do Parlamento da CEDEAO.

#### **ADOA:**

### **ARTIGO 1: ADOÇÃO DE MEDIDAS DE REFORÇO DA CONFIANÇA (MRC)**

A presente **DIRETIVA C/DIR. 2/12/24** adota o primeiro conjunto de Medidas de Reforço da confiança (MRC) da seguinte forma:

- 1. MRC nº1. Partilhar informações sobre documentação relacionada com cibersegurança**
  - a. O Estado-membro deve ser encorajado a partilhar informações com outros Estados-membros sobre as suas políticas, estratégias, regulamentação, melhores práticas, perceções de ameaças e programas nacionais de cibersegurança, no formato e nas instâncias escolhidos, conforme

adequado.

- b. Sempre que possível e aplicável, o Estado-membro fornecedor pode declarar ou destacar um possível alinhamento da documentação, informação ou melhores práticas partilhadas aplicadas em toda a região da CEDEAO.

## **2. MRC nº 2. Designar pontos de contato nacional**

- a. Cada Estado-membro deve:
  - i. designar pontos de contacto diplomáticos e técnicos para apoiar a coordenação da comunicação e dos debates sobre cibersegurança a nível nacional, regional e internacional;
  - ii. ser encorajado a assegurar a coordenação a nível nacional entre os pontos de contato;
  - iii. ser encorajado a fornecer e atualizar regularmente os dados de contato dos seus pontos de contato designados;
  - iv. ser encorajado a estabelecer medidas para assegurar intercâmbios rápidos e atempados em caso de incidentes de cibersegurança nacionais ou internacionais;
  - v. encorajado a designar os seus pontos de contacto em conformidade com as listas das Nações Unidas estabelecidas a nível mundial.
- b. Estes pontos de contato coordenam as respostas, de natureza diplomática ou técnica, e facilitam as interações entre os respetivos organismos nacionais;
- c. A Comissão da CEDEAO deve servir como facilitador da rede de pontos de contato.

## **3. MRC nº 3. Aumentar a sensibilização para as ciber ameaças e medidas de reparação**

- a. O Estado-membro deve ser encorajado a facilitar ou participar em atividades colaborativas para aumentar a sensibilização e melhorar a preparação contra as ameaças à cibersegurança nos respetivos países e na região.
- b. As atividades referidas na alínea a) supra, podem ser dirigidas a entidades nacionais de cibersegurança, a peritos ou ao público. Estas atividades colaborativas podem incluir, mas não estão limitadas a:
  - i. Campanhas nas redes sociais com componentes escrita e audiovisual;
  - ii. Entrevistas e notificações na rádio, televisão ou *online*;
  - iii. Mesas redondas com especialistas dirigidas a públicos-alvo;
  - iv. Realização de campanhas impressas de sensibilização;
  - v. Comissionamento e distribuição de materiais destinados a combater ameaças específicas decorrentes do ciberespaço.

- c. Os Estados-membros devem reforçar as capacidades cibernéticas, nomeadamente através de reuniões, conferências e partilha de conhecimentos.
- d. Os Estados-membros devem continuar a trocar pontos de vista no âmbito dos grupos de peritos sobre o desenvolvimento e a aplicação de mecanismos de cooperação transfronteiriça, incluindo o potencial desenvolvimento de adicionais MRC.

## **ARTIGO 2: CRIAÇÃO DO GRUPO DE TRABALHO DE CIBERSEGURANÇA DA CEDEAO**

1. Os Estados-membros devem ser encorajados a criar um grupo de trabalho informal e aberto, composto por peritos nacionais em cibersegurança de todos os Estados-membros da CEDEAO num prazo de três (3) meses após a entrada em vigor da presente Diretiva.

O grupo de trabalho deve ser presidido pelo perito do Estado-membro que preside a Autoridade dos Chefes de Estado e de Governo.

2. O grupo de trabalho deve ser encorajado a reunir-se anualmente para debater os progressos realizados, partilhar pontos de vista e planejar iniciativas futuras.
3. A Comissão da CEDEAO deve funcionar como secretariado e apoiar o presidente na realização das seguintes tarefas:
  - a. elaborar medidas individuais de reforço de confiança destinadas a reforçar a transparência, a cooperação, a previsibilidade e as capacidades necessárias para reduzir os riscos de escalada, mal-entendidos e conflitos decorrentes da utilização do ciberespaço/TIC;
  - b. aprovar MRC elaboradas por consenso e, quando for o caso, submetê-las à adoção;
  - c. adotar Medidas de Reforço da Confiança com indicadores e medições de sucesso;
  - d. discutir as modalidades de implementação e operacionalização das medidas de reforço da confiança adotadas pelos Estados-membros da CEDEAO;
  - e. apresentar relatórios anuais ao Conselho de Ministros sobre os progressos realizados na adoção e implementação de Medidas de Reforço da Confiança, em conformidade com os indicadores de sucesso;
  - f. conduzir discussões orientadas pelos seguintes princípios:
    - i. todas as Medidas de Reforço de Confiança devem ser aplicáveis de forma igual a todos os Estados-membros, sem discriminação com base na capacidade de cibersegurança, geografia, nacionalidade ou na língua;
    - ii. embora voluntária, todas as Medidas de Reforço de Confiança adotadas devem ser compreendidas e aceites a nível de cada Estado-membro; e

- iii. as Medidas de Reforço da Confiança devem ser sincronizadas com as medidas regionais e iniciativas nacionais destinadas a reforçar a ciber-resiliência, capacidades e segurança na região da CEDEAO;
4. O Estado Membro deve reconhecer que as Medidas de Reforço da Confiança são adotadas e devem funcionar num ambiente multilateral com atores governamentais, não governamentais, do setor privado e outros atores ativos na cibersegurança na região da CEDEAO.

### **ARTIGO 3: REVISÃO**

1. A presente Diretiva deve ser revista e alterada conforme necessário para mitigar os riscos identificados ou para incluir outras MRC identificadas.
2. A Diretiva pode igualmente ser revista sob recomendação dos Chefes das Instituições da Comunidade.

### **ARTIGO 4: PUBLICAÇÃO**

1. A presente **DIRETIVA C/DIR. 2/12/24** deve ser publicada pela Comissão no Jornal Oficial da Comunidade no prazo de trinta (30) dias a contar da data da sua assinatura pelo Presidente do Conselho de Ministros.
2. Deve ser igualmente publicada por cada Estado-membro no seu jornal oficial dentro do mesmo prazo.

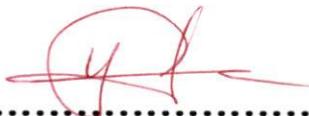
### **ARTIGO 5: ENTRADA EM VIGOR**

A presente **DIRETIVA C/DIR. 2/12/24** entra em vigor a partir da sua publicação.

**FEITO EM ABUJA, NO DIA 13 DE DEZEMBRO DE 2024**

**PELO CONSELHO**

**O PRESIDENTE**



.....  
**S.E. EMB. YUSUF MAITAMA TUGGAR (OON)**