



## PRIORIDADES DE SEGURANÇA NO CIBERESPAÇO PARA OS ATORES DA SEGURANÇA NACIONAL DE ÁFRICA

### NOTA INFORMATIVA

**O QUÊ:** O Centro África facilitará um programa virtual de quatro semanas para examinar o papel dos atores de segurança nacional na resposta aos desafios de segurança do ciberespaço em África. Este programa discutirá como o setor da segurança pode cooperar com outros intervenientes dos setores público e privado para enfrentar as crescentes ameaças cibernéticas no continente. Os participantes que completarem o curso receberão o respetivo certificado.

Os objetivos do programa são os seguintes:

1. Melhorar a compreensão das ameaças e desafios de segurança do ciberespaço na África.
2. Identificar prioridades para os atores Africanos de defesa e segurança a considerar quando se prepararem e responderem contra as atividades cibernéticas maliciosas.
3. Comparar experiências, perspectivas e boas práticas na política de segurança do ciberespaço numa série de setores de segurança civis, privado e intervenientes não governamentais.

**ONDE:** Online, via Zoom para o Governo

**QUANDO:** 3-4 de agosto de 2021  
10-11 de agosto de 2021  
17-18 de agosto de 2021  
24-25 de agosto de 2021

**QUEM:** Indivíduos com um vasto leque de contextos no setor de segurança, governo, setor privado e sociedade civil serão convidados a participar. Os seguintes países são convidados a nomear participantes: Argélia, Angola, Benim, Botsuana, Burkina Faso, Burundi, Cabo Verde, República Centro Africana, Chade, Comores, Congo, República Democrática do Congo, Costa do Marfim, Djibuti, Egipto, Eswatini, Gabão, Gâmbia, Gana, Guiné, Guiné-Bissau, Quênia, Lesoto, Libéria, Líbia, Madagáscar, Malawi, Mali, Mauritânia, Maurícias, Marrocos, Moçambique, Namíbia,

Níger, Nigéria, Ruanda, São Tomé e Príncipe, Senegal, Seicheles, Serra Leoa, Somália, África do Sul, Sudão, Tanzânia, Togo, Tunísia, Zâmbia. Cada país é convidado a nomear três participantes: pelo menos um dos quais deve ser do setor de segurança uniformizado; pelo menos um deve ser civil; e pelo menos um deve ser do sexo feminino. Serão convidados outros participantes de comunidades econômicas regionais, organizações multilaterais e acadêmicas, bem como alguns representantes do governo dos EUA.

Os participantes devem ser funcionários de nível médio a superior, tenentes-coronéis ou equivalente e superior, de preferência ocupando cargos responsáveis pela segurança cibernética ou política e estratégia tecnológica emergente. Exemplos de possíveis nomeados incluem:

- oficiais da força aérea ou da inteligência militar que procuram defender os seus países contra as ameaças da tecnologia emergente;
- polícia e gendarmes de unidades de ameaça cibernética ou de inteligência financeira responsáveis por recolher provas forenses digitais ou de investigar crimes digitais; e
- funcionários públicos, nomeados, ou peritos técnicos de alto nível que trabalham em política e estratégia cibernética para gabinetes do presidente, ministérios dos negócios estrangeiros, ministérios das telecomunicações, consultores de segurança nacional e/ou equipas de resposta a incidentes informáticos (CIRTs).

**PORQUÊ:** A crescente penetração da Internet e a rápida inovação na tecnologia digital está a amplificar e a mudar a natureza dos desafios de segurança de uma série de atores estatais, não estatais e criminosos em toda a África. O setor de segurança tem um papel crucial a desempenhar na proteção de infraestruturas nacionais críticas contra ataques cibernéticos e na resposta aos usos maliciosos das tecnologias de informação por parte de atores organizados e violentos. Uma política eficaz de segurança do ciberespaço requer a cooperação entre as partes interessadas.

**COMO:** Este compromisso virtual combinará conversas plenárias ao vivo (90 minutos) e grupos de discussão semanais não presenciais (90 minutos). Os participantes serão convidados a rever as leituras e vídeos de webinars cibernéticos anteriores antes da realização do programa.

O programa será composto por quatro sessões:

- 1) Panorama da Ameaça do Espaço Cibernético na África
- 2) Elementos chave de uma resposta nacional de segurança no ciberespaço
- 3) Segurança Cibernética de Infraestruturas Críticas

4) Estratégias de Segurança Nacional e de Segurança do Ciberespaço

O programa será conduzido em Inglês, Francês e Português.