# OCTOGÉSIMA QUINTA SESSÃO ORDINÁRIA DO CONSELHO DE MINISTROS DA COMUNIDADE ECONÓMICA DOS ESTADOS DA ÁFRICA OCIDENTAL

VÍDEOCONFERÊNCIA, 20-21 de janeiro de 2021

## DIRETIVA C/DIR.1/01/2021 QUE ADOTA A ESTRATÉGIA REGIONAL DE CIBERSEGURANÇA E DE LUTA CONTRA A CIBERCRIMINALIDADE

## O Conselho de Ministros,

**TENDO EM CONTA** os artigos 10.º, 11.º e 12.º do Tratado da CEDEAO na redação vigente, que criam o Conselho de Ministros e definem a sua composição e as suas funções;

**TENDO EM CONTA** os artigos 27.º, 32.º e 33.º de referido Tratado sobre a ciência e a tecnologia e sobre os domínios de comunicações e telecomunicações;

**TENDO EM CONTA** o Ato Adicional A/SA.1/01/07 da CEDEAO sobre a harmonização das políticas e do quadro regulamentar do setor das Tecnologias da Informação e Comunicação (TiC);

**TENDO EM CONTA** o Ato Adicional A/SA.1/01/10 sobre a proteção dos dados de caráter pessoal no espaço CEDEAO;

**TENDO EM CONTA** o Ato Adicional A/SA.2/01/10 sobre as transações eletrónicas no espaço CEDEAO;

**TENDO EM CONTA** a Diretiva C/DIR/1/08/11 sobre a luta contra a cibercriminalidade no espaço CEDEAO,

**CONSIDERANDO** que a utilização das Tecnologias da Informação e Comunicação entre as quais a Internet ou a cibernética continua a gerar um recrudescimento de atos repreensíveis de toda a ordem;

**CONSIDERANDO** a necessidade de ajudar os Estados-membros da Comunidade a reforçar as suas capacidades de cibersegurança e a proteger os seus ciberespaços e as suas infraestruturas de informação críticas;

**CONSCIENTE** da importância de adotar uma abordagem regional coordenada para aniquilar os impactos nocivos dos ciberataques e da cibercriminalidade e reforçar o ecossistema da cibersegurança a fim de proteger o espaço CEDEAO;

**DESEJOSO** de adotar no espaço CEDEAO uma estratégia regional de cibersegurança e de luta contra a cibercriminalidade;

**SOB RECOMENDAÇÃO** da décima sétima Reunião dos Ministros responsáveis pelo setor das Telecomunicações/TIC e dos Correios realizada por videoconferência de 23 a 25 de novembro de 2020;

**APÓS PARECER** do Parlamento da Comunidade aquando da segunda Sessão Ordinária, por videoconferência, de 13 a 29 de janeiro de 2021;

**ACORDA NO SEGUINTE :**

**ARTIGO 1.º**

A Estratégia regional de cibersegurança e de luta contra a cibercriminalidade, em anexo, é adotada.

**ARTIGO 2.º**

A presente Diretiva **C/DIR. 1/01/2021** entra em vigor na data da sua assinatura pelo Presidente do Conselho de Ministros.

**ARTIGO 3.º**

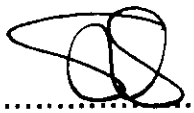
1. A presente Diretiva **C/DIR. 1/01/2021** será publicada pela Comissão da CEDEAO no Jornal oficial da Comunidade no prazo de trinta (30) dias contados da data da sua assinatura pelo Presidente do Conselho de Ministros.

2. Ainda a presente Diretiva **C/DIR. 1/01/2021** será publicada no mesmo prazo por cada Estado-membro da CEDEAO no respetivo Boletim oficial.

**Feito no dia 21 de janeiro de 2021**

**Pelo Conselho de Ministros**

**A Presidente**



.....

**Sua Excelência a Senhora Shirley Ayorkor Botchwey**


# Estratégia Regional de Ciber segurança e de Luta Contra a Cibercriminalidade da CEDEAO

## Sumário

## SECÇÃO I. INTRODUÇÃO

A rápida transformação digital que ocorre na África Ocidental é de grande importância para melhorar o funcionamento e a eficiência das administrações, das políticas públicas e das economias, assim como para aumentar o bem-estar das populações. No entanto, os riscos crescentes que ameaçam o ciberespaço mundial e as redes digitais, os sistemas de informação e dados, podem reduzir significativamente os benefícios esperados dessas políticas numéricas e prejudicar seriamente os interesses das nações, das suas economias, das suas instituições e dos seus povos.

Diante dessas ameaças e riscos, devem ser implementados fortes sistemas nacionais de cibersegurança e de luta contra o cibercrime, com boa coordenação entre os departamentos envolvidos, bem como mecanismos eficazes de resposta a ataques cibernéticos, com especialistas e usuários do digital competentes e treinados em boas práticas, a participação ativa do setor privado, a proteção aprimorada dos serviços e infraestruturas numéricas mais essenciais ou críticas, bem como a assistência mútua regional e a cooperação internacional.

É claro que na região esses requisitos ainda estão longe de serem cumpridos. Se alguns países já adotaram as providências necessárias e alcançaram um certo grau de preparação, a maioria dos outros países ainda tem um nível insuficiente de preparação, constituindo isso uma fraqueza que põe em perigo as suas nações tanto quanto o restante da região. Além disso, todos os países enfrentam escassez de perícia nessas áreas. Por isso, são incentivados a desenvolver cursos de treinamento em ciber segurança e a atingir um nível mínimo em segurança cibernética e na luta contra o crime cibernético.

Além disso, a heterogeneidade dos dispositivos existentes nos diferentes países limita consideravelmente qualquer tentativa de cooperação regional. Deve procurar-se, portanto, uma harmonização: vínculos e trocas seriam mais fáceis e mais eficazes entre instituições com perímetros de responsabilidade e modos de operação semelhantes; requisitos e procedimentos idênticos garantiriam a proteção da infraestrutura transnacional da mesma maneira em toda a região; finalmente, disposições harmonizadas de procedimentos penais e criminais tornariam possível a verdadeira assistência jurídica mútua.

Nesta área, a CEDEAO implementou disposições de harmonização desde 2010: o ato adicional A/SA.1/01/10, relativo à proteção de dados pessoais no espaço da CEDEAO, estabelece, em particular, as obrigações de segurança que incumbem aos responsáveis pelo tratamento desses dados para garantir a confidencialidade; o ato adicional A/SA.2/01/10, relativo às transações eletrónicas na região da CEDEAO, fixa as condições para a aceitação da assinatura eletrónica; por fim, a Diretiva C/DIR/1/08/11 sobre a luta contra o cibercrime na região da CEDEAO adapta o direito penal e o procedimento penal dos Estados Membros ao fenómeno do cibercrime.

A nível continental, a Convenção da União Africana de 2014 sobre a Ciber segurança e Proteção de Dados Pessoais, conhecida como Convenção de Malabo, estabelece as medidas de ciber segurança e de luta contra os crimes cibernéticos a serem adotadas a nível nacional. A nível mundial, a Convenção de 2001 sobre a Cibercriminalidade, conhecida como Convenção de Budapeste, aberta à assinatura de todos os países, visa implementar uma política criminal comum adotando legislação adequada para intensificar a cooperação entre Estados-Membros em matéria penal e adotar poderes suficientes para permitir uma luta eficaz contra o cibercrime.

O objetivo desta Estratégia Regional é aproveitar ao máximo esses avanços, melhorar o nível dos sistemas nacionais de ciber segurança e de luta contra o cibercrime, e desenvolver a cooperação e a assistência mútua entre os países da região. Baseia-se nas melhores práticas internacionalmente reconhecidas nessas áreas.

Esses objetivos devem ser alcançados sem prejuízo das liberdades fundamentais e dos direitos do homem e dos povos contidos nas declarações, convenções e outros instrumentos adotados aos níveis regional, continental e internacional.

## SECÇÃO II. DISPOSIÇÕES GERAIS

### A. Objetivo geral

O objetivo geral dessa estratégia regional é criar o quadro estratégico da Comunidade a ser analisado pelos Estados-Membros em suas estratégias nacionais e a ser implementado em seus planos de ação sobre segurança cibernética e luta contra o crime cibernético antes do final de 2022, com participação plena da Comissão da CEDEAO em benefício dos Estados-Membros desta Comunidade.

### B. Definições

No âmbito desta Estratégia Regional, aplicam-se as seguintes definições:

**Infraestrutura crítica**: uma infraestrutura ou processo público ou privado cuja destruição, paralisação, exploração ilegítima ou perturbação durante um período de tempo definido causará perda de vidas ou perda significativa para a economia ou prejudicará significativamente a reputação do Estado-Membro ou os seus símbolos de governação. Nesta definição, as infraestruturas incluem as redes, os sistemas e os dados físicos ou digitais essenciais para a prestação deste serviço. Este termo pode referir-se a um determinado sistema ou processo cujo funcionamento é crítico dentro da organização;

**Operador de infraestruturas críticas**: operador público ou privado que opera uma infraestrutura crítica;

**Proteção de infraestruturas críticas (PIC)**: conjunto de salvaguarda e ações para proteger as infraestruturas críticas de quaisquer riscos e ameaças que possam causar a interrupção total ou parcial dos serviços essenciais por elas prestados.

**CSIRT (*Computer Security Incident Response Team*)**: equipa responsável por prevenir riscos e ameaças aos sistemas de informação e reagir em caso de incidentes de segurança e fornecer ajuda na mitigação;

**Higiene informática:** todas as boas práticas que cada ator do digital deve respeitar para preservar a segurança do sistema de informações que usa ou para o qual atua como administrador;

**Cibercriminalidade**: atividades criminosas nas quais computadores e sistemas informáticos são a arma ou o principal alvo. O cibercrime abrange os crimes habituais (fraude, falsificação, usurpação de identidade, etc.), crimes vinculados a conteúdo (arquivos de pornografia infantil, incitação ao ódio racial, etc.) e crimes específicos a computadores e sistemas informáticos (ataque contra um sistema informático, negação de serviço, aplicativo malicioso...);

**Ciberespaço**: rede interdependente de infraestruturas que utilizam tecnologias da informação, incluindo nomeadamente a Internet, redes de telecomunicações, sistemas de informação e objetos conectados;

**Ciber segurança**: todas as medidas e ações destinadas a proteger o ciberespaço contra ameaças associadas às suas redes e infraestrutura informática ou que possam danificá-las. A ciber segurança visa preservar a disponibilidade e a integridade das redes e infraestruturas, bem como a confidencialidade das informações nelas contidas;

**Dados numéricos**: qualquer representação de factos, informações ou conceitos sob qualquer forma que se presta ao processamento informático;

**Infraestrutura crítica:** infraestrutura pública ou privada que fornece um serviço essencial, bem como os dados físicos ou numéricos necessários para a prestação desse serviço;

**Operador de infraestrutura crítica:** operador público ou privado que opera uma infraestrutura crítica;

**Operador de serviço essencial**: operador público ou privado que presta um serviço essencial;

**Proteção das infraestruturas críticas**: todas as medidas e ações destinadas a proteger as infraestruturas críticas de todos os riscos e ameaças que possam causar a interrupção total ou parcial dos serviços essenciais que fornecem;

**Proteção de serviços essenciais:** todas as medidas e ações destinadas a proteger os serviços essenciais de todos os riscos e ameaças que possam causar a sua interrupção total ou parcial;

**Serviço essencial:** serviço cuja interrupção total ou parcial pode ter um sério impacto no funcionamento do Governo, na economia do país ou na saúde, na segurança e bem-estar dos cidadãos;

**Redes:** todos os meios para garantir o fornecimento de uma infraestrutura em produtos ou serviços necessários para o seu funcionamento (comunicações, energia, logística, etc.);

**Sistema de informação:** qualquer dispositivo isolado ou não, qualquer conjunto de dispositivos interconectados que garantam na totalidade ou em parte um processamento automatizado de dados na execução de um programa;

**Tecnologias da informação e da comunicação (TIC):** tecnologias usadas para coletar, armazenar, usar e enviar informações, incluindo aquelas que envolvem o uso de computadores ou qualquer sistema de comunicação, incluindo telecomunicações.

## SECÇÃO III. OBJETIVO ESTRATÉGICO 1 : FORMULAR UMA POLÍTICA NACIONAL E UMA ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA E DE LUTA CONTRA A CIBERCRIMINALIDADE

Cada Estado-Membro deve adotar e atualizar, pelo menos a cada 5 anos, uma política nacional e uma estratégia nacional de ciber segurança e de luta contra o cibercrime[1] levando em consideração a presente Estratégia Regional e estabelecendo para cada das duas áreas:

- A situação do país e seus desafios;
- A visão política do país;
- Os objetivos estratégicos a alcançar, os prazos e as prioridades;
- A governança e as responsabilidades;
- Os objetivos em termos:
    - de reforço das disposições legislativas e regulamentares;
    - de normas, padrões e referenciais de exigências;
    - de segurança das infraestruturas críticas e serviços essenciais;
    - de reforço de quadro institucional;
    - de competências técnicas e recursos humanos qualificados a serem adquiridos;
    - de sensibilização, de comunicação, de educação e de formação;
    - de prevenção de ameaças e gestão de riscos;
    - de sinalização de incidentes de segurança;
    - de deteção e de atribuição dos ataques;
    - de reação em caso de ataque;
    - de desenvolvimento de um ecosistema de ciber segurança e de luta contra a cibercriminalidade;
    - de sinergia de ações à escala nacional, de concertação e de coordenação nacional;
    - de cooperação regional e internacional;
- As ações a serem realizadas para alcançar esses objetivos, os intervenientes, os prazos e os orçamentos estimados;
- Os meios destinados a fortalecer instituições e capacidades e a garantir a sua sustentabilidade.

Cada Estado-Membro deve definir um mecanismo de acompanhamento e avaliação, pelo menos anualmente, das ações previstas na sua estratégia nacional de ciberseguranca e de luta contra o cibercrime.

[1] A política nacional e a estratégia nacional podem ser objeto de documentos separados ou de um único documento de estratégia nacional que estabeleça a visão e os objetivos políticos do país.

## SECÇÃO IV. OBJETIVO ESTRATÉGICO 2 : REFORÇAR A CIBERSEGURANÇA COM UM CIBERESPAÇO SEGURO E FIÁVEL

Reforçar a ciber segurança através de um ciber espaço seguro e protegido

### Sub-objetivo 2.1. Estabelecer uma autoridade nacional de ciber segurança

Cada Estado-Membro deve estabelecer e designar uma autoridade nacional de ciber segurança com os poderes e os meios necessários para desempenhar as seguintes funções, diretamente ou por delegação de uma autoridade governamental, de preferência interministerial[2]:

- A governança global do sistema nacional de ciber segurança (definição da política nacional e das políticas setoriais de ciber segurança, desenvolvimento da estratégia nacional e das estratégias setoriais, acompanhamento dos planos de ação, preparação de textos legislativos e regulamentares, coordenação das tarefas relacionadas com a ciber segurança, pilotagem dos dispositivos de prevenção e resposta, facilitação de intercâmbios entre as partes interessadas públicas e privadas, etc.);
- A animação do sistema nacional de ciber segurança, em particular através da CSIRT nacional;
- A coordenação com as autoridades responsáveis da luta contra a cibercriminalidade;
- A transposição de atos comunitários na área da ciber segurança para textos nacionais;
- O controlo da boa aplicação das convenções internacionais, dos atos comunitários, da presente estratégia regional e das disposições legislativas e regulamentares nacionais na área da ciber segurança;
- O papel do principal ponto de contacto para a cooperação regional e internacional.

A autoridade nacional de ciber segurança deverá poder exercer a sua missão em todos os setores de atividade do país (serviços estatais, telecomunicações, energia, saúde, transporte, bancos, etc.), em conjunto com as autoridades setoriais competentes e sem prejuízo dos poderes dessas autoridades.

### Sub-objetivo 2.2. Estabelecer as Capacidades de alerta e resposta em caso de incidente (CSIRT)

Cada Estado-Membro deverá ter uma CSIRT nacional:

- Devendo cobrir em prioridade os serviços de Estado-Membro, as infraestruturas críticas e os serviços essenciais (os "beneficiários prioritários") ;
- Responsável por animar e coordenar a rede das CSIRT setoriais, se houver, buscando todas as sinergias e complementaridades possíveis;
- Capaz de executar pelo menos as seguintes funções:
    - A pesquisa e a difusão de alertas (vulnerabilidade, riscos, incidentes), medidas de evasão de ameaças, guias e boas práticas;
    - O acompanhamento de incidentes a nível nacional;
    - O tratamento de incidentes afetando os beneficiários prioritários;
    - A participação na rede regional e na rede mundial das CSIRT;
    - A Coordenação de respostas e gestão de crise em contacto com as autoridades em caso de um ataque importante;
    - A aquisição de serviços de informação relevantes;
    - A integração de sistemas e tecnologias relevantes para recolher e analisar rapidamente os dados relevantes;
    - A criação de um centro de chamadas para comunicar os ciber ataques;

[2] No entanto, recomenda-se que os Estados-membros mais pequenos e médios estabeleçam uma autoridade central, que trabalhe com todos os outros ministérios devido à falta de recursos, às rápidas mudanças e à necessidade de estar atualizado, uma vez que, por vezes, a criação de grandes comités interministeriais pode dificultar o progresso.

- Dotada dos meios necessários (financeiros, locais e sistema de informação seguros, efetivo suficiente para garantir uma disponibilidade permanente, pessoal competente, competências na área forense, procedimentos, site internet, etc.).

Cada Estado-Membro deverá incentivar a constituição de CSIRT setoriais, destinadas a assegurar de maneira comum, para o benefício dos operadores em certos setores de atividade, a pesquisa e a divulgação de alertas sobre sistemas e aplicativos numéricos para esses setores de atividade e tratamento de incidentes. Recomenda-se que as CSIRT se situem no mesmo local para assegurar um diálogo aberto e um enriquecimento inter setorial.

**Sub-objetivo 2.3. Implementar uma abordagem de gestão de riscos**

Cada Estado-Membro deverá adotar ou fazer adotar uma abordagem de gestão de riscos, tanto a nível estratégico quanto a nível dos órgãos públicos e privados, a fim de garantir com equidade o nível necessário de segurança das redes, sistemas de informação e dados numéricos.

Cada Estado-Membro deverá garantir aos responsáveis de ciber segurança, seja qual for o nível, o apoio hierárquico necessário para que as suas análises e recomendações sejam levadas em consideração pelos decisores.

**Sub-objetivo 2.4. Reforçar a ciber segurança das infraestruturas críticas e dos serviços essenciais**

Cada Estado-Membro deverá priorizar os seus esforços de ciber segurança nas suas infraestruturas críticas e serviços essenciais.

Cada Estado-Membro deverá estabelecer um procedimento para identificar redes, sistemas de informação e dados numéricos essenciais para o funcionamento das infraestruturas críticas e a prestação de serviços essenciais.

Cada Estado-Membro deverá impor aos operadores públicos e privados responsáveis pelas infraestruturas críticas e serviços essenciais algumas medidas concretas para garantir a segurança dessas redes, sistemas de informação e dados numéricos, incluindo as seguintes medidas mínimas:

- o cumprimento das medidas de higiene informática;
- uma auditoria de segurança dos sistemas de informação por um organismo qualificado, com uma frequência não superior a dois anos;
- a notificação de incidentes de segurança à autoridade nacional de ciber segurança ou à CSIRT nacional (através de sua possível CSIRT setorial).

**Sub-objetivo 2.5. Adotar políticas de segurança dos sistemas de informação**

Cada Estado-Membro deverá impor aos serviços de Estado e aos operadores das infraestruturas críticas e serviços essenciais, e recomendar aos outros operadores, o desenvolvimento e aplicação das políticas de segurança descritas nas disposições previstas para garantir a segurança dos seus sistemas de informação (responsabilidades, organização, recursos humanos dedicados, equipamentos de ciber segurança, procedimentos de proteção, de deteção e de reação aos ataques, etc.).

**Sub-objetivo 2.6. Estabelecer um referencial geral de segurança**

Cada Estado-Membro deverá estabelecer um referencial geral de segurança que defina os requisitos mínimos para a segurança dos sistemas de informação (governança, organização, política de segurança dos sistemas de informação, mapeamento dos sistemas, requisitos técnicos, etc.) e designar as organizações a ele sujeitas num documento com caráter jurídico.

**Sub-objetivo 2.7. Garantir o desenvolvimento de competências na área da cibersegurança**

Cada Estado-Membro deverá garantir a formação de recursos humanos suficientes nos vários aspetos da ciber segurança:

- Introduzindo cursos de formação nas diversas áreas relacionadas com a ciber segurança (técnica, jurídica, etc.) nos seus programas de ensino, em particular no ensino universitário e profissional;
- Promovendo o reforço das competências de ciber segurança entre todos os profissionais das Tecnologias da Informação e Comunicação ;
- Incentivando a pesquisa e a inovação na área da ciber segurança;
- Integrar requisitos de conhecimentos comprovados em matéria de ciber segurança nos concursos públicos para os serviços.

**Sub-objetivo 2.8. Garantir o desenvolvimento do ecossistema da ciber segurança**

Cada Estado-Membro deverá garantir e promover a criação de organizações públicas e privadas capazes de prestar assistência a operadores em matéria da cibersegurança (fornecimento de soluções seguras, proteção de sistemas de informação, consultoria, auditoria, tratamento de incidentes, etc.).

## SECÇÃO V. OBJETIVO ESTRATÉGICO 3 : REDUZIR A CIBERCRIMINALIDADE ATRAVÉS DE UM AMBIENTE ADEQUADO E A CAPACIDADE DE APRESENTAR OS INFRATORES À JUSTIÇA

**Sub-objetivo 3.1. Adotar disposições penais e procedimentos penais**

Cada Estado-Membro deverá adotar as disposições penais e processuais prescritas ou recomendadas, aos níveis regional, continental e mundial.

Cada Estado deverá adotar sanções adequadas para as infrações penais que afetaram ou tentaram afetar os sistemas de informação e dados necessários para o bom funcionamento das infraestruturas críticas e dos serviços essenciais.

**Sub-objetivo 3.2. Implementar capacidades de luta contra o cibercrime**

Cada Estado-Membro deverá ter as seguintes capacidades mínimas de luta contra a cibercriminalidade:

- Pelo menos uma unidade operacional de luta contra a cibercriminalidade;
- Uma autoridade coordenadora se tiver várias unidades de luta contra a cibercriminalidade;
- Pelo menos um laboratório de investigação;
- Recursos de recolha de provas numéricas;
- Procedimentos para a investigação, recolha e tratamento de provas numéricas;
- Investigadores do Estado-Membro (oficiais e agentes da polícia judicial, especialistas jurídicos, etc) formados em investigações numéricas, na recolha e tratamento de provas numéricas;
- Magistrados formados na instrução e julgamento de casos relacionados com a cibercriminalidade.

## SECÇÃO VI. OBJETIVO ESTRATÉGICO 4: PROMOVER A COORDENAÇÃO E A COOPERAÇÃO EM CIBER CRIMINALIDADE

**Sub-objetivo 4.1. Promover A ratificação das Convenções**

Cada Estado-Membro deverá ratificar as Convenções regionais, continentais e internacionais necessárias sobre a ciber segurança e a luta contra a cibercriminalidade.

**Sub-objetivo 4.2. Assegurar a promoção da cultura de ciber segurança**

Cada Estado-Membro deverá promover uma cultura da ciber segurança usando todos os meios possíveis (comunicação governamental, seminários, meios de comunicação, formação nas escolas e universidades e ainda a formação contínua, etc.) para alcançar os seguintes objetivos:

- A sensibilização de todos sobre as ameaças cibernéticas;
- A promoção da higiene informática e outras boas práticas numéricas junto do grande público;
- A sensibilização dos decisores públicos e privados sobre os seus papéis e suas responsabilidades;
- Alertar os cidadãos sobre as sanções para atos de cibercriminalidade.

**Sub-objetivo 4.3. Assegurar a coordenação nacional**

Os Estados-Membros deverão mobilizar todos os intervenientes públicos e privados para promover e desenvolver consultas, coordenação e sinergias entre todas as partes interessadas, em particular:

- autoridades e instituições responsáveis pela ciber segurança ou luta contra a cibercriminalidade;
- operadores de infraestruturas críticas;
- fornecedores de produtos de ciber segurança ou produtos seguros;
- prestadores de serviços de ciber segurança;
- instituições de formação e pesquisa;
- organizações da sociedade civil;
- meios de comunicação.

**Sub-objetivo 4.4. Promover a cooperação regional e internacional**

Os Estados-Membros e a Comissão da CEDEAO deverão promover e desenvolver a cooperação regional e internacional entre autoridades e instituições responsáveis pela ciber segurança e luta contra a cibercriminalidade:

- No domínio do desenvolvimento de capacidades: em particular pela partilha de boas práticas e pela busca de sinergias e da mutualização intra regional, em particular no domínio da formação;
- No campo institucional: para harmonizar as estratégias, organizações e procedimentos dos países da região, em particular no que diz respeito à ciber segurança das infraestruturas críticas transnacionais e à luta contra a cibercriminalidade;
- Na área operacional: para partilhar alertas e informações sobre ciber segurança entre CSIRT nacionais e para organizar respostas conjuntas ou até reunir meios de intervenção para combater, da maneira mais eficaz possível, as ameaças cibernéticas potenciais ou comprovadas e o cibercrime;
- No campo judicial: para prestar assistência jurídica mútua em cibercriminalidade e garantir o acesso transnacional a provas numéricas;
- Criar um centro regional de simulação e formação em ciber segurança para reduzir os custos e promover a interoperabilidade;
- Incentivar organizações conjuntas de partilha de informação nos serviços críticos e essenciais (energia, finanças, saúde, etc.);
- Criar mecanismos e memorandos de entendimento conjuntos com outras organizações de partilha de informação.

## SECÇÃO VII. OBJETIVO ESTRATÉGICO 5: ESTABELECER MECANISMOS REGIONAIS

**Sub-objetivo 5.1. Estabelecer um plano de assistência regional para a implementação da estratégia regional**

A fim de ajudar os Estados-Membros na aplicação desta Estratégia Regional, a Comissão da CEDEAO implementará, com os meios à sua disposição, o plano de ação regional que figura no anexo.

**Sub-objetivo 5.2. Estabelecer um dispositivo de acompanhamento da estratégia regional**

A Comissão da CEDEAO estudará com os Estados-Membros a conveniência de estabelecer um Comitê Técnico Regional (CTR / RTC, *Regional Technical Committee*) duradouro, composto por um representante de alto nível fornecido por cada Estado-Membro, sob a coordenação da Comissão da CEDEAO e que se reúne, pelo menos, uma vez por ano, para garantir ao longo do tempo o acompanhamento das disposições desta estratégia e propor as novas ações necessárias.

**Sub-objetivo S.3. Estabelecer um centro de coordenação da cibersegurança**

A Comissão da CEDEAO estudará com os Estados-Membros a oportunidade de criar a curto ou médio prazo, um centro de coordenação de ciber segurança para a CEDEAO, que irá coordenar as várias iniciativas de capacitação realizadas nos diversos países no domínio da ciber segurança e da luta contra o cibercrime, e organizar, sempre que possível, a recolha e a partilha de resultados entre países.

O centro de coordenação da ciber segurança poderá, a longo prazo, implementar uma agência regional responsável por promover e liderar a cooperação regional no domínio da cibersegurança e da luta contra o cibercrime.

**Sub-objetivo 5.4. Identificar e procurar financiamento para dispositivos nacionais de ciber segurança e de luta contra o cibercrime**

A Comissão da CEDEAO estudará com os Estados-Membros as possibilidades de harmonizar, dentro da CEDEAO, mecanismos de financiamento para dispositivos nacionais de ciber segurança e de luta contra a cibercriminalidade, particularmente no que diz respeito a impostos e parcerias público-privadas.

A Comissão da CEDEAO, em contato com os Estados-Membros, buscará financiamento junto aos doadores para atender às necessidades prioritárias não atendidas desses Estados-Membros.