Sexta-feira, 29 de janeiro de 2021

I Série
Número 9

BOLETIM OFICIAL

ÍNDICE

CONSELHO DE MINISTROS

Decreto-lei nº 9/2021

de 29 de janeiro

A segurança cibernética assume atualmente um papel tão importante como a segurança no espaço físico, sendo, cada vez mais, uma componente fundamental da Segurança Nacional, a um passo que as Tecnologias de Informação e Comunicação (TIC) se tornaram um elemento verdadeiramente crucial de suporte às atividades do quotidiano.

No cenário atual em que se verifica um crescimento da dependência das organizações em relação a sistemas informáticos, mas também um aumento dos ataques cibernéticos, a conjugação desses dois fatores faz com que as consequências dos ataques cibernéticos sejam cada vez mais graves, desde a perda ou roubo de dados críticos até a interrupção do negócio, provocando grandes perdas em termos de confiança na organização e em termos financeiros.

Assim sendo, todos os países estão a adotar medidas e políticas orientadas para o incremento da cibersegurança, tanto na componente preventiva como na componente de resposta a incidentes, especialmente aqueles que constituem crimes de natureza patrimonial, mas também pondo em causa bens jurídicos pessoais, nomeadamente a privacidade, a identidade de cada cidadão, no que é hoje denominado cibercrime, nas suas mais diferentes e complexas modalidades.

A efetiva securização das TIC, à semelhança de outras já consideradas críticas, como as redes de distribuição de energia elétrica ou a rede telefónica pública, reveste-se da maior importância.

Para que Cabo Verde possa garantir um ambiente seguro também na sua sociedade de informação, no domínio da governação eletrónica, na prestação de um número crescente de serviços públicos facilitados e mais próximos do cidadão e prevenir e combater o cibercrime, é necessário que sejam desenvolvidas ações com vista a implementar recomendações internacionais, bem assim como os eixos de intervenção estabelecidos na Estratégia Nacional de Cibersegurança (ENCS), aprovada pela Resolução n.º 21/2016, de 7 de março, dos quais se destacam:

a) Criar consciência, no seio da sociedade de informação, sobre a necessidade de realizar ações nacionais e desenvolver cooperação internacional no âmbito da Cibersegurança;

b) Identificar os papéis e as responsabilidades dos atores nos processos de cooperação interinstitucional necessários para a Cibersegurança;

c) Desenvolver e aplicar políticas nacionais que obedeçam a recomendações internacionais sobre a matéria, de forma a alcançar uma maior resiliência cibernética e desenvolver capacidades de prevenir, investigar e punir o cibercrime.

A referida estratégia prevê, desde logo, uma estrutura de coordenação, que, a um passo, cuide da sua implementação e lance as bases para o que virá a ser o Centro Nacional de Cibersegurança, que terá por missão, garantir que Cabo Verde usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como para a Equipa de Resposta a Incidentes de Segurança Informática (acrónimo em inglês - Computer Security Incident Response Team-CSIRT).

O diploma tem um âmbito necessariamente abrangente, que abrange a Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais, os prestadores de serviços digitais, em suma quaisquer entidades que utilizem redes e sistemas de informação, sejam públicas ou privadas.

O processo de elaboração do presente diploma foi coordenada por uma comissão nomeada pelo Primeiro Ministro, da qual participaram a Direção-Geral das Telecomunicações e Economia Digital (DGTED), o Núcleo Operacional da Sociedade de Informação (NOSI), a Agência Reguladora Multisectorial da Economia (ARME), a Direção Geral da Polícia Judiciária (DGPJ), o Sistema Nacional de Identificação e Autenticação Civil (SNIAC) e o Gabinete de Segurança Nacional.

Foram ouvidos e absorvidas as recomendações constantes dos pareceres emitidos pela ARME e pela Comissão Nacional de Proteção de Dados, tendo-se também recebido contribuições de empresas diretamente implicadas, nomeadamente da CV Telecom.

Assim,

No uso da faculdade conferida pela alínea *a*) do artigo 204º da Constituição, o Governo decreta o seguinte:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1º

Objeto

1- O presente diploma estabelece o regime jurídico cabo-verdiano para a cibersegurança, destinado a garantir um elevado nível de segurança das redes e dos sistemas de informação em Cabo Verde.

2- O presente diploma adota as Diretivas C/DIR. 1/08/11 da Comunidade Económica dos Estados da África Ocidental (CEDEAO), visando a sua gradual convergência normativa com as comunidades, organizações e demais Estados com os quais Cabo Verde mantém cooperação nesta matéria.

Artigo 2º

Âmbito

1- O presente diploma aplica-se:

a) À Administração Pública;

b) Aos operadores de infraestruturas críticas;

c) Aos operadores de serviços essenciais;

d) Aos prestadores de serviços digitais;

e) A quaisquer outras entidades que utilizem redes e sistemas de informação, sejam públicas ou privadas.

2- A aplicação do presente diploma, nomeadamente, quanto ao tratamento, responsabilidade e proteção de dados pessoais, observa o regime jurídico geral de proteção de dados pessoais das pessoas singulares.

3- O presente diploma aplica-se:

a) À Administração Pública direta;

b) Às autarquias locais;

c) Às entidades administrativas independentes;

d) Aos institutos públicos;

e) Às empresas públicas;

f) Às associações públicas.

4- O presente diploma aplica-se aos prestadores de serviços digitais que tenham o seu estabelecimento principal em território nacional ou, não o tendo, designem um representante estabelecido em território nacional, desde que aí prestem serviços digitais.

5- Para efeitos do número anterior, considera-se que um prestador de serviços digitais tem o seu estabelecimento principal em território nacional quando aí tiver a sua sede.

6- Caso uma entidade se enquadre simultaneamente em mais do que uma das alíneas *a*) a *c*) do n.º 1, aplica-se o regime que resultar mais exigente para a segurança das redes e dos sistemas de informação.

7- O presente diploma aplica-se ainda, sem prejuízo de legislação ou regulamentação específica que venha a ser aprovada:

a) Às redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas;

b) Às redes e sistemas de informação que processem informação classificada.

8- O presente diploma não prejudica as medidas destinadas a salvaguardar as funções essenciais do Estado, incluindo medidas de proteção da informação cuja divulgação seja contrária aos interesses de segurança nacional, à manutenção de ordem pública ou a permitir a investigação, a deteção e a repressão de infrações penais.

Artigo 3º

Definições

Para efeitos do presente diploma, entende-se por:

a) «Ciberespaço», ambiente complexo de valores e interesses materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas e redes e sistemas de informação;

b) «Cibersegurança», conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem;

c) «Equipa de Resposta a Incidentes de Segurança Informática ou *Computer Security Incident Response Team* (CSIRT)», a equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação;

d) «Especificação técnica», um documento que define os requisitos técnicos que um produto, processo, serviço ou sistema devem cumprir;

e) «Gestão de Eventos de Segurança ou *Security Information and Event Management* (SIEM)», usa regras e correlações estatísticas para transformar entradas de log e eventos de uma ampla variedade de fontes de dados em informações que possam ajudar as equipas de segurança;

f) «Incidente», um evento com um efeito adverso real na segurança das redes e dos sistemas de informação;

g) «Infraestrutura crítica», a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções;

h) «Norma», uma especificação técnica, aprovada por um organismo de normalização reconhecido, para aplicação repetida ou continuada, cuja observância não é obrigatória;

i) «Operador de infraestrutura crítica», uma entidade pública ou privada que opera uma infraestrutura crítica;

j) «Operador de serviços essenciais», uma entidade pública ou privada que presta um serviço essencial;

k) «Ponto de troca de tráfego», uma estrutura de rede que permite a interligação de mais de dois sistemas autónomos independentes a fim de facilitar a troca de tráfego na *Internet;*

l) «Prestador de serviços digitais», uma pessoa coletiva que presta um serviço digital;

m) «Prestador de serviços do sistema de nomes de domínio», uma entidade que presta serviços do sistema de nomes de domínio (DNS) na *Internet*;

n) «Rede de comunicações eletrónicas», os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos que permitem o envio de sinais por cabo, meios radioelétricos, meios óticos, ou por outros meios eletromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, os sistemas de cabos de eletricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes utilizadas para a radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida);

o) «Registo de nomes de domínio de topo», uma entidade que administra e opera o registo de nomes de domínio da *Internet* de um domínio de topo específico;

p) «Representante do prestador de serviços digitais», uma pessoa singular ou coletiva, estabelecida em Cabo Verde, expressamente designada para atuar por conta de um prestador de serviços digitais aí não estabelecido;

q) «Risco», uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação;

r) «Segurança das redes e dos sistemas de informação», a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles;

s) «Serviço de computação em nuvem», um serviço digital que permite o acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis;

t) «Serviço de mercado em linha», um serviço digital que permite aos consumidores ou aos comerciantes celebrarem contratos de compra e venda ou de prestação de serviços por via eletrónica com comerciantes, quer no sítio na *Internet* do mercado em linha, quer no sítio na *Internet* de um comerciante que utilize os serviços de computação disponibilizados pelo mercado em linha;

u) «Serviço de motor de pesquisa em linha», um serviço digital que permite aos utilizadores consultarem todos os sítios na *Internet*, ou sítios na *Internet* numa determinada língua, com base numa pesquisa sobre qualquer assunto e que fornece ligações onde podem ser encontradas informações relacionadas com o conteúdo solicitado;

v) «Serviço digital», um serviço da sociedade da informação prestado à distância, por via eletrónica;

w) «Serviço essencial», um serviço essencial para a manutenção de atividades societárias ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço;

x) «Sistema de Gestão de Incidentes ou *Incident Management System* (IMS)» é uma ferramenta que permite organizar o processo de resposta a incidentes, sendo parte da infraestrutura do CSIRT;

y) «Sistema de nomes de domínio» (DNS), um sistema de nomes distribuídos hierarquicamente numa rede que encaminha pesquisas sobre nomes de domínio;

z) «Tratamento de incidentes», todos os procedimentos de apoio à deteção, análise, contenção e resposta a um incidente.

Artigo 4º

Estratégia Nacional de Cibersegurança

1- A Estratégia Nacional para a Cibersegurança, define o enquadramento, os objetivos estratégicos e as linhas de ação do Estado de Cabo Verde nesta matéria, de acordo com o interesse nacional.

2- A Estratégia Nacional para a Cibersegurança é aprovada e revista por Resolução do Conselho de Ministros, ouvida o Núcleo Nacional de Cibersegurança.

3- A Estratégia Nacional para a Cibersegurança é revista quinquenalmente.

CAPÍTULO II

ESTRUTURA DE SEGURANÇA DO CIBERESPAÇO

Artigo 5º

Núcleo Nacional de Cibersegurança

1- O Núcleo Nacional de Cibersegurança é o órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço.

2- Os membros do Núcleo Nacional de Cibersegurança são designados por Resolução do Conselho de Ministros, que designa, de entre os membros designados, aquele que Preside, podendo ser determinada a rotatividade no exercício da função.

3- O presidente, por sua iniciativa ou a pedido de qualquer dos membros do Núcleo, pode convocar outros titulares de órgãos públicos, de entidades privadas ou convidar outras personalidades de reconhecido mérito para participar em reuniões do Núcleo Nacional de Cibersegurança.

Artigo 6º

Competências do Núcleo Nacional de Cibersegurança

1- Compete ao Núcleo Nacional de Cibersegurança:

a) Assegurar a coordenação político-estratégica para a segurança do ciberespaço;

b) Supervisionar a implementação da Estratégia Nacional de Segurança do Ciberespaço;

c) Pronunciar-se sobre a Estratégia Nacional de Segurança do Ciberespaço, previamente à sua submissão para aprovação ou revisão;

d) Elaborar anualmente, ou sempre que necessário, relatório de avaliação da execução da Estratégia Nacional de Cibersegurança;

e) Propor ao Primeiro-Ministro, ou ao membro do Governo em quem este delegar, a aprovação de decisões de carácter programático relacionadas com a definição e execução da Estratégia Nacional de Cibersegurança;

f) Emitir parecer sobre matérias relativas à cibersegurança;

g) Responder a solicitações por parte do Primeiro-Ministro, ou do membro do Governo em quem este delegar, no âmbito das suas competências;

h) Acompanhar e emitir pareceres e recomendações sobre a criação, instalação e definir as competências e funcionamento do Centro Nacional de Cibersegurança.

2- O relatório anual de avaliação da execução da Estratégia Nacional de Cibersegurança é enviado ao Conselho de Ministros até 31 de março do ano posterior àquele a que se reporta.

Artigo 7º

Centro Nacional de Cibersegurança

1- O Centro Nacional de Cibersegurança funciona, sem prejuízo da sua autonomia financeira e administrativa, junto ao Gabinete de Segurança Nacional e corresponde à Autoridade Nacional de Cibersegurança.

2- O Centro Nacional de Cibersegurança tem por missão garantir que Cabo Verde usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais.

3- O Centro Nacional de Cibersegurança é o ponto de contacto único nacional para efeitos de cooperação internacional, sem prejuízo das atribuições legais da Procuradoria Geral da República e da Polícia Judiciária, relativas a cooperação internacional em matéria penal.

Artigo 8º

Atribuições e competências

1- São atribuições do Centro Nacional de Cibersegurança:

a) Exercer as funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias, nos termos a regulamentar em diploma próprio;

b) Emitir instruções de cibersegurança e definir o nível nacional de alerta de cibersegurança;

c) Solicitar a quaisquer entidades públicas ou privadas toda a colaboração ou auxílio que julgue necessários para o exercício das suas atividades;

d) Atuar em articulação com a Comissão Nacional de Proteção de Dados quando estejam em causa incidentes que tenham dado origem à violação de dados pessoais;

e) Realizar auditorias externas às entidades e instituições abrangidas pelo presente diploma, por iniciativa própria ou mediante solicitação das autoridades judiciárias, quando entender necessário, nos termos a regulamentar;

f) Propor ao Governo a celebração e revisão de acordos, protocolos ou contratos com entidades públicas ou privadas nacionais ou internacionais, incluindo as entidades congéneres do exterior, que se mostrem adequados à elevação dos padrões de Cibersegurança do país.

2- Qualquer disposição legal relativa à matéria de cibersegurança carece do parecer prévio do Centro Nacional de Cibersegurança.

Artigo 9º

Equipa de Resposta a Incidentes de Segurança Informática

1- A Equipa de Resposta a Incidentes de Segurança Informática (CSIRT.CV) funciona na dependência orgânica do Centro Nacional de Cibersegurança

2- A organização e funcionamento da CSIRT.CV é regulamentado em diploma próprio.

Artigo 10º

Competências do CSIRT.CV

O CSIRT.CV, sem prejuízo de outras atribuições que lhe podem ser acometidas, possui as seguintes competências:

a) Exercer a coordenação operacional na resposta a incidentes, nomeadamente em articulação com as equipas de resposta a incidentes de segurança informática setoriais existentes;

b) Monitorizar os incidentes com implicações a nível nacional;

c) Ativar e emitir mecanismos de alerta rápido sobre incidentes de Cibersegurança;

d) Intervir na reação, análise e mitigação de incidentes;

e) Proceder à análise dinâmica dos riscos;

f) Assegurar a cooperação com entidades públicas e privadas;

g) Promover a adoção e a utilização de práticas comuns ou normalizadas;

h) Participar e assegurar a representação nacional nos *foruns* nacionais e internacionais de cooperação de equipas de resposta a incidentes de segurança informática;

i) Participar em eventos de treino nacionais e internacionais;

j) Proceder à classificação dos incidentes de Cibersegurança por níveis de gravidade e definir os procedimentos de alerta e resposta de acordo com esses níveis.

Artigo 11º

Operadores de serviços essenciais

1- Os operadores de serviços essenciais enquadram-se num dos tipos de entidades que atuam nos setores e subsetores constantes do anexo ao presente diploma e que dele faz parte integrante.

2- Os prestadores de serviços essenciais, devem realizar um registo formal junto ao CSIRT.CV, sem prejuízo da privacidade, do âmbito de atuação e das competências que são atribuídas ao Centro Nacional de Cibersegurança previstas no n.º 2 do artigo 7º.

Artigo 12º

Prestadores de serviços digitais

Os prestadores de serviços digitais são os que prestam os seguintes serviços:

a) Serviço de mercado em linha;

b) Serviço de motor de pesquisa em linha;

c) Serviço de computação em nuvem; e

d) Outros que operam no setor da economia digital.

CAPÍTULO III

SEGURANÇA DAS REDES E DOS SISTEMAS DE INFORMAÇÃO

Artigo 13º

Definição de requisitos de segurança e normalização

1- Os requisitos de segurança são definidos nos termos previstos em regulamentação própria, sem prejuízo do disposto no artigo 19º, cabendo ao Centro Nacional de Cibersegurança, definir as políticas de segurança para os sistemas de informação, nomeadamente, a definição de responsabilidades em segurança cibernética, estrutura da organização, recursos humanos dedicados, equipamentos, procedimentos de proteção, deteção e resposta a ataques.

2- A aprovação dos regulamentos a que se refere o número anterior estão dependentes de parecer prévio da Comissão Nacional de Proteção de Dados.

3- Os requisitos de segurança são definidos de forma a permitir a utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.

Artigo 14º

Definição de requisitos de notificação de incidentes

1- Os requisitos de notificação de incidentes são definidos nos termos previstos em regulamentação própria, sem prejuízo do disposto no artigo 20º.

2- A aprovação do regulamento a que se refere o número anterior está dependente do parecer prévio da Comissão Nacional de Proteção de Dados.

Artigo 15º

Requisitos de segurança para a Administração Pública e operadores de infraestruturas críticas

1- A Administração Pública e os operadores de infraestruturas críticas, independentemente da sua natureza pública ou privada, particularmente aquelas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas, acessíveis ao público devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, sendo aplicáveis os requisitos de segurança previstas no diploma que estabelece as políticas, normas e regras de segurança de informação para a gestão da Rede Tecnológica Privativa do Estado (RTPE).

2- As medidas previstas no número anterior devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.

3- A Administração Pública e os operadores de infraestruturas críticas tomam as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados e para reduzir ao mínimo o seu impacto.

4- Para efeitos de disposto no n.º 1, o Centro Nacional de Cibersegurança aprova as medidas técnicas de execução para aplicação pelos operadores de infraestruturas críticas.

Artigo 16º

Notificação de incidentes para a Administração Pública e operadores de infraestruturas críticas

1- A Administração Pública e os operadores de infraestruturas críticas notificam o Centro Nacional de Cibersegurança dos incidentes com um impacto relevante na segurança das redes e dos sistemas de informação, no prazo definido em regulamentação própria referida no artigo 14º.

2- A notificação dos operadores de infraestruturas críticas inclui informação que permita ao Centro Nacional de Cibersegurança determinar o impacto transfronteiriço dos incidentes.

3- A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4- A fim de determinar a relevância do impacto de um incidente são tidos em conta, designadamente, os seguintes parâmetros:

a) O número de utilizadores afetados;

b) A duração do incidente;

c) A distribuição geográfica, no que se refere à zona afetada pelo incidente.

5- O Centro Nacional de Cibersegurança deve prestar ao notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente informações que possam contribuir para o tratamento eficaz do incidente, exceto quando as circunstâncias o impeçam.

6- O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar incidentes específicos de acordo com o interesse público, salvaguardando a segurança e os interesses dos operadores de infraestruturas críticas.

7- Para efeitos do disposto no n.º 1, compete ao Centro Nacional de Cibersegurança aprovar as medidas que definam as circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade, mediante parecer prévio da Comissão Nacional de Proteção de Dados.

Artigo 17º

Requisitos de segurança para os operadores de serviços essenciais

1- Os operadores de serviços essenciais devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.

2- As medidas previstas no número anterior devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.

3- Os operadores de serviços essenciais tomam as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados para a prestação dos seus serviços essenciais e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços.

4- Os operadores de serviços essenciais realizam obrigatoriamente auditorias internas anuais até ao dia 31 de dezembro do ano a que disser respeito, produzindo delas um Relatório, que é remetido ao Centro Nacional de Segurança, no prazo máximo de 15 dias, a contar da data da conclusão da auditoria.

Artigo 18º

Notificação de incidentes pelos operadores de serviços essenciais

1- Os operadores de serviços essenciais notificam o Centro Nacional de Cibersegurança dos incidentes com um impacto relevante na continuidade dos serviços essenciais por si prestados, no prazo definido em regulamentação própria a que se refere o artigo 13º

2- A notificação inclui informação que permita ao Centro Nacional de Cibersegurança determinar o impacto transfronteiriço dos incidentes.

3- A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4- A fim de determinar a relevância do impacto de um incidente são tidos em conta, designadamente, os seguintes parâmetros:

a) O número de utilizadores afetados pela perturbação do serviço essencial;

b) A duração do incidente;

c) A distribuição geográfica, no que se refere à zona afetada pelo incidente.

5- Com base na informação prestada, o Centro Nacional de Cibersegurança informa os pontos de contacto únicos de outros Estados afetados, caso o incidente tenha um impacto importante na continuidade dos serviços essenciais desses Estados.

6- Nos casos referidos no número anterior, o Centro Nacional de Cibersegurança salvaguarda a segurança e os interesses do operador de serviços essenciais, bem como a confidencialidade da informação prestada na sua notificação.

7- O Centro Nacional de Cibersegurança deve prestar ao notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente informações que possam contribuir para o tratamento eficaz do incidente, exceto quando as circunstâncias o impeçam.

8- O Centro Nacional de Cibersegurança transmite as notificações referidas no n.º 1 aos pontos de contacto únicos dos outros Estados que ratificaram os instrumentos internacionais de que Cabo Verde também faz parte.

9- O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar informação relativa a incidentes específicos de acordo com o interesse público.

10- Se um operador de serviços essenciais depender de um terceiro prestador de serviços digitais para a prestação de um serviço essencial, notifica todos os impactos importantes na continuidade dos seus serviços, decorrentes dos incidentes que afetem o prestador de serviços digitais.

11- Para efeitos do disposto no n.º 1, compete ao Centro Nacional de Cibersegurança aprovar as medidas que definam as circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade.

Artigo 19º

Requisitos de segurança para os prestadores de serviços digitais

1- Os prestadores de serviços digitais identificam e tomam as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam no contexto da oferta dos serviços digitais.

2- As medidas referidas no número anterior devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes, e devem ter em conta os seguintes fatores:

a) A segurança dos sistemas e das instalações;

b) O tratamento dos incidentes;

c) A gestão da continuidade das atividades;

d) O acompanhamento, a auditoria e os testes realizados;

e) A conformidade com as normas internacionais.

3- A fim de assegurar a sua continuidade, os prestadores de serviços digitais tomam medidas para evitar os incidentes que afetem a segurança das suas redes e sistemas de informação e para reduzir ao mínimo o seu impacto nos serviços digitais.

Artigo 20º

Notificação de incidentes para os prestadores de serviços digitais

1- Os prestadores de serviços digitais notificam o Centro Nacional de Cibersegurança dos incidentes com impacto substancial na prestação dos serviços digitais, no prazo mais curto possível para o tratamento dos dados, atendendo aos parâmetros enunciados no n.º 4.

2- A notificação referida no número anterior inclui informação que permita ao Centro Nacional de Cibersegurança determinar a importância dos impactos transfronteiriços.

3- A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4- A fim de determinar se o impacto de um incidente é substancial, são tidos em conta os seguintes parâmetros:

a) O número de utilizadores afetados pelo incidente, nomeadamente de utilizadores que dependem do serviço para prestarem os seus próprios serviços;

b) A duração do incidente;

c) A distribuição geográfica, no que se refere à zona afetada pelo incidente;

d) O nível de gravidade da perturbação do funcionamento do serviço;

e) A extensão do impacto nas atividades económicas e societais.

5- A obrigação de notificar um incidente só se aplica se o prestador de serviços digitais tiver acesso a informação necessária para avaliar o impacto de um incidente em função dos fatores a que se refere o n.º 2 do artigo anterior.

6- Se os incidentes referidos no n.º 1 disserem respeito a dois ou mais Estados, o Centro Nacional de Cibersegurança informa os pontos de contacto únicos dos outros Estados afetados.

7- Nos casos a que se refere o número anterior, o Centro Nacional de Cibersegurança salvaguarda a segurança e os interesses do prestador de serviços digitais.

8- O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar incidentes específicos de acordo com o interesse público.

9- Para efeitos do disposto no n.º 1, compete ao Centro Nacional de Cibersegurança aprovar as medidas que definam as circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade, mediante parecer obrigatório da Comissão Nacional de Proteção de Dados.

Artigo 21º

Notificação voluntária de incidentes

1- Sem prejuízo da obrigação de notificação de incidentes prevista no presente diploma, quaisquer entidades podem notificar, a título voluntário, os incidentes com impacto importante na continuidade dos serviços por si prestados.

2- No tratamento das notificações voluntárias, aplica-se o disposto no artigo 18º, com as necessárias adaptações.

3- A notificação voluntária não pode dar origem a quaisquer imposições à entidade notificante de obrigações às quais esta não teria sido sujeita se não tivesse procedido a essa notificação.

CAPÍTULO IV
FISCALIZAÇÃO E SANÇÕES

Artigo 22º

Competências de fiscalização e sancionatórias

As competências de fiscalização e de aplicação das sanções previstas no presente diploma cabem ao Centro Nacional de Cibersegurança.

Artigo 23º

Contraordenações

As infrações ao disposto no presente diploma constituem contraordenações, nos termos dos artigos seguintes.

Artigo 24º

Infrações muito graves

1- Constituem infrações muito graves:

a) O incumprimento da obrigação de implementar requisitos de segurança prevista nos artigos 15º, 17º e 19º;

b) O incumprimento de instruções de cibersegurança emitidas pelo Centro Nacional de Cibersegurança tal como previsto na al. *b*) do no n.º 1 do artigo 8º.

2- As contraordenações referidas no número anterior são punidas com coima de 50.000$00 (cinquenta mil escudos) a 300.000$00 (trezentos mil escudos), tratando-se de uma pessoa singular, e de 150.000$000 (cento e cinquenta mil escudos) a 1.000.000$00 (um milhão de escudos), no caso de se tratar de uma pessoa coletiva.

Artigo 25º

Infrações graves

1- Constituem infrações graves:

a) O incumprimento da obrigação de notificar o Centro Nacional de Cibersegurança dos incidentes prevista nos artigos 16º, 18º e 20º;

b) O incumprimento da obrigação de notificar o Centro Nacional de Cibersegurança do exercício de atividade no setor das infraestruturas digitais prevista no n.º 3 do artigo 30º;

c) O incumprimento da obrigação de notificar o Centro Nacional de Cibersegurança da identificação como prestador de serviços digitais prevista no artigo 31º.

2- As contraordenações referidas no número anterior são punidas com coima de 20.000$00 (vinte mil escudos) a 80.000$00 (oitenta mil escudos), tratando-se de uma pessoa singular, e de 80.000$00 (oitenta mil escudos) a 250.000$00 (duzentos e cinquenta mil escudos), no caso de se tratar de uma pessoa coletiva.

Artigo 26º

Negligência

A negligência é punível, sendo os limites mínimos e máximos das coimas reduzidos a metade.

Artigo 27º

Instrução dos processos de contraordenação e aplicação de sanções

Compete ao Centro Nacional de Cibersegurança instruir os processos de contraordenação e ao respetivo dirigente máximo a aplicação das coimas.

Artigo 28º

Produto das coimas

O produto das coimas reverte em:

a) 60 % para o Estado; e

b) 40 % para o Centro Nacional de Cibersegurança.

Artigo 29º

Regime subsidiário

Em tudo o que não estiver previsto no presente diploma, aplica-se o disposto no regime geral das contraordenações.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Artigo 30º

Identificação de operadores de serviços essenciais

1- Para efeito do cumprimento do presente diploma, o Centro Nacional de Cibersegurança identifica os operadores de serviços essenciais no prazo de um ano a contar da data da sua instalação.

2- A identificação referida no número anterior é objeto de atualização anual.

3- Uma vez instalado o Centro Nacional de Cibersegurança, as entidades do setor das infraestruturas digitais devem comunicar-lhe de imediato o início do exercício da respetiva atividade.

Artigo 31º

Identificação de prestadores de serviços digitais

Uma vez instalado o Centro Nacional de Cibersegurança, os prestadores de serviços digitais devem comunicar-lhe de imediato o início do exercício da respetiva atividade.

Artigo 32º

Legislação complementar

1- Os requisitos de segurança previstos no n.º 1 do artigo 15º, no n.º 1 do artigo 17º e no n.º 1 do artigo 19º são definidos em diploma próprio no prazo de cento e cinquenta dias a contar da data da entrada em vigor do presente diploma.

2- Os requisitos de notificação de incidentes previstos no n.º 1 do artigo 16º, no n.º 1 do artigo 18º e no n.º 1 do artigo 20º são definidos em diploma próprio no prazo de cento e cinquenta dias a contar da data da entrada em vigor do presente diploma.

Artigo 33º

Produção de efeitos

Sem prejuízo do disposto no artigo seguinte, os regimes constantes dos artigos 16º a 28º produzem efeitos no prazo de cento e oitenta dias, a contar da data da instalação do Centro Nacional de Cibersegurança.

Artigo 34º

Entrada em vigor

O presente diploma entra em vigor no prazo de cento e oitenta dias a contar da data da sua publicação.

Aprovado em Conselho de Ministros, aos 17 de dezembro de 2020. — Os Ministros, *José Ulisses de Pina Correia e Silva, Olavo Avelino Garcia Correia* e *Paulo Augusto Rocha*

Promulgado em 27 de janeiro de 2021

Publique-se.

O Presidente da República, JORGE CARLOS DE ALMEIDA FONSECA.

ANEXO

(A que se refere o artigo 11º)

OPERADORES DE SERVIÇOS ESSENCIAIS

Sector	Subsector	Tipo de Entidade
Energia	Eletricidade	Empresa de eletricidade que exerce a atividade de produção ou de comercialização
		Operadores da rede de distribuição
		Operadores da rede de transporte
	Petróleo	Operadores de oleodutos de petróleo
		Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo
	Gás	Empresas de comercialização
		Operadores da rede de distribuição
		Operadores da rede de transporte
		Operadores do sistema de armazenamento
		Operadores da rede de gás natural em estado líquido (GNL).
		Empresas de gás natural
		Operadores de instalações de refinamento e tratamento de gás natural
Transportes	Transporte aéreo	Transportadoras aéreas, companhias, agentes, operadores
		Entidades gestoras aeroportuárias, aeroportos e as entidades que exploram instalações anexas existentes dentro dos aeroportos.
		Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo.
	Transporte marítimo e por Vias navegáveis interiores	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias.
		Entidades gestoras dos portos, incluindo as respetivas instalações portuárias e as entidades que gerem as obras e os equipamentos existentes dentro dos portos.
		Operadores de serviços de tráfego marítimo.
	Transporte rodoviário	Autoridades rodoviárias.
		Operadores de sistemas de transporte inteligentes.
Bancário	--	Instituições de crédito.
		Operadores de plataformas de negociação.
Infraestruturas do mercado financeiro	--	Contrapartes centrais.
Saúde	Instalações de prestação de cuidados de saúde	Prestadores de cuidados de saúde.
Fornecimento e distribuição de água potável.	--	Fornecedores e distribuidores de água destinada ao consumo humano, mas excluindo os distribuidores para os quais a distribuição de água para consumo humano é apenas uma parte da sua atividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais.
Infraestruturas digitais e de telecomunicação	--	Pontos de troca de tráfego.
		Prestadores de serviços de Sistema de Nomes de Domínio (DNS).
		Registos de nomes de domínio de topo.
		Operadores de telecomunicação.
		Rede Tecnológica Privativa do Estado

Decreto-Regulamentar nº 1/2021

de 29 de janeiro

As CSIRT (acrónimo em inglês para *Computer Security Incident Response Team* - Equipa de Resposta a Incidentes de Segurança Informática) são equipas ou entidades centralizadas, que têm como principais objetivos a prevenção, identificação, gestão e resolução de problemas relacionados com a segurança informática de forma rápida e eficiente.

No cenário atual em que se verifica um crescimento da dependência das organizações em relação a sistemas informáticos e um aumento dos ataques cibernéticos, a conjugação desses dois fatores fazem com que as consequências dos ataques cibernéticos sejam cada vez mais graves, desde a perda ou roubo de dados críticos até a interrupção do negócio, provocando grandes perdas em termos de confiança na organização e em termos financeiros. A segurança cibernética assume atualmente um papel tão importante como a segurança no espaço físico, assumindo cada vez mais como uma componente fundamental da segurança nacional, uma vez que as TIC (Tecnologias de Informação e Comunicação) se tornaram um elemento verdadeiramente crucial de suporte às atividades do quotidiano.

É assim que todos os países estão a adotar medidas e políticas orientadas para o incremento da cibersegurança, tanto na componente preventiva como na componente de resposta a incidentes, especialmente aqueles que constituem crimes, o cibercrime. A efetiva securização das TIC, à semelhança de outras já consideradas críticas como as redes de distribuição de energia elétrica ou a rede telefónica pública, se revista da maior importância.

Neste contexto, os serviços de resposta a incidentes de segurança informática têm sido apontados como essenciais na prevenção e reação ao fenômeno da cibercriminalidade. Assim sendo, a implementação de um CSIRT permite à organização centralizar a monitorização de todos os ativos de tecnologias e sistemas de informação (redes, servidores, base de dados, aplicações, entre outros) e manter o ambiente seguro, detetando e respondendo a incidentes de forma rápida e metódica e posteriormente fazendo uma investigação e relato detalhado, possibilitando a tomada de medidas preventivas com base nas conclusões.

Neste regime, são especificados os requisitos necessários para a implementação e regulamentação de CSIRT.CV, começando pelos objetivos e tarefas que definem o que se espera de um CSIRT em termos de resultados práticos e em termos de funções desempenhadas, passando pelo requisitos em termos de infraestrutura, ou seja, o SIEM (Security Information and Event Management ou Gestão de Eventos de Segurança), o IMS (Incident Management System ou Sistema de Gestão de Incidentes) e o espaço físico do CSIRT, em termos de recursos humanos, nomeadamente as responsabilidades e competências necessárias das três equipas do CSIRT (equipa de monitorização e análise, equipa de resposta a incidentes e equipa de cibersegurança), em termos dos procedimentos para fazer a monitorização, deteção, análise e escalonamento, mitigação/resolução, forense e prevenção de incidentes, e por fim, é especificado a política de segurança da informação recomendada pela FIRST (Forum of Incident Response and Security Teams).

O presente diploma foi elaborado, tendo em linha de conta as boas práticas e recomendações na matéria, emanadas da ENISA (European Network and Information Security Agency) e da RFC (Request For Comments) 2350, procurando-se, numa matéria cuja convergência normativa reveste-se de especial importância, criar uma estrutura que possa ser assumida no contexto nacional e reconhecida pelos parceiros internacionais, particularmente importantes no que à ciber-segurança diz respeito.

Pese embora a estrutura da equipa CSIRT faça sentido num quadro mais abrangente de intervenção no espaço de cibersegurança nacional, qual seja a criação de um Centro Nacional de cibersegurança, em que tal equipa seja um dos seus departamentos, a sua criação antecipada justifica-se pela prioridade na assunção das funções que se lhe acometem, impondo-se que, o quanto antes, o país seja dotada de uma equipa competente e apetrechada para responder e mitigar a ataques ou outros incidentes cibernéticos, cada ve mais frquentes e com cada vez maior potencial lesivo, mormente para um país que investiu seriamente numa administração pública desmaterializada e que pretende que a sua economia também o seja. Outrossim, o impacto que a pandemia da Covid-19 teve na busca de soluções assentes nas tecnologias de comunicação para a realização de um número cada vez maior de tarefas, em que, entre outros, os dados pessoais dos cidadãos são cada vez mais transacionados, nomeadamente no incremeto exponencial do comércio eletrónico.

Efetivamente, será a aprovação do presente diploma que irá permitir a instalação do CSIRT, através da mobilização de rescursos técnicos, humanos e financeiros, mormemente de projetos internacionais, do Banco Mundial e da CEDEAO, que permitirão que esta seja uma das primeiras prioridades elencadas na Estratégia Nacional de Cibersegurança desenhada para o país, a ser materializada, para então se irem criando condições para a instalação paulatina do Centro Nacional de Cibersegurança, do qual passará a ser um departamento funcional.

A nível de estrutura administrativa, é, pois, consagrado um regime transitório, que permite que a equipa que ora se cria possa ter um enquadramento proviório e funcional, enquanto núcleo de missão, até que possa vir a ser transferida para a estrutura do Centro Nacional de Cibersegurança, quando este vier a ser criado e instalado, aprovando-se nessa altura o necessário Plano de Cargos, Carreiras e Salários. Entretanto, prevê-se que a estrutura física da equipa funcione, autonomamente, no *datacenter* governamental, sob gestão do NOSi, que partilhará a gestão administrativa e financeira do CSIRT.CV com uma comissão nomeada para o efeito, escolhida de entre os integrantes do Núcleo Nacional para a Cibersegurança, previsto nos na Resolução 21/2016, de 7 de março, cujos representantes devem ser nomeados, nos termos dos seus artigos 4º e 5º, no prazo máximo de 30 dias, a contar da aprovação do presente diploma.

É ainda previsto que, uma vez aprovado o presente diploma, se venha a aprovar o regulamento de funcionamento e de procedimentos do CSIRT.CV.

Considerando a matéria, bem como o fato de se pretender a criação de uma nova estrutura na administração direta do Estado, foram solicitados os pareceres da Comissão Nacional de Proteção de Dados, cujo parecer foi devidamente absorvido, tendo-se ainda solicitado os necessários pareceres da Administração Pública e Finanças, tendo-se ultrapassado, entretanto, o prazo regimental obrigatório, sem que tenham sido enviados.

Assim,

Nos termos dos artigos 9º e 10º do Regime Jurídico de Cibersegurança;

No uso da faculdade conferida pela alínea *b*) do artigo 205º e pela alínea *a*) do n.º 2 do artigo 264º da Constituição, o Governo decreta o seguinte:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1º

Objeto

1- O presente diploma procede à criação da Equipa de Resposta a Incidentes de Segurança Informática, define as suas funções e estrutura, bem como o seu enquadramento administrativo.

2- A Equipa de Resposta a Incidentes de Segurança Informática nacional é denominada de CSIRT.CV, cujo objetivo é prestar serviços de monitorização, deteção, resposta e prevenção de incidentes informáticos, centralizando a monitorização dos ativos de tecnologias de informação e agindo de forma tanto preventiva como reativa para garantir a confidencialidade, integridade e disponibilidade dos dados e das comunicações.

Artigo 2º

Âmbito

1- O presente diploma aplica-se:

a) À Administração Pública;

b) Aos operadores de infraestruturas críticas;

c) Aos operadores de serviços essenciais;

d) Aos prestadores de serviços digitais;

e) A quaisquer outras entidades que utilizem redes e sistemas de informação.

2- Para efeitos do disposto no presente diploma, integram a Administração Pública:

a) A Administração Pública;

b) As autarquias locais;

c) As entidades administrativas independentes; e

d) As associações públicas.

3- O presente diploma aplica-se aos prestadores de serviços digitais que tenham o seu estabelecimento principal em território nacional ou, não o tendo, designem um representante estabelecido em território nacional, desde que aí prestem serviços digitais.

4- Para efeitos do número anterior, considera-se que um prestador de serviços digitais tem o seu estabelecimento principal em território nacional quando aí tiver a sua sede.

5- Caso uma entidade se enquadre simultaneamente em mais do que uma das alíneas *a*) a *c*) do n.º 1, aplica-se o regime que resultar mais exigente para a segurança das redes e dos sistemas de informação.

6- O presente diploma aplica-se ainda, sem prejuízo de legislação ou regulamentação específica que venha a ser aprovada:

a) Às redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas;

b) Às redes e sistemas de informação que processem informação classificada.

7- O previsto no presente diploma presupõe o cumprimento da legislação aplicável em matéria de proteção de dados pessoais, designadamente a Lei n.º 133/V/2011, de 22 de janeiro, suas alterações e regulamentos associados e das demais normas em vigor relativas à proteção de dados pessoais.

Artigo 3º

Definições

Para efeitos do presente diploma aplicam-se as definições consagradas no Regime Jurídico de Cibersegurança.

CAPÍTULO II

FUNÇÃO E ESTRUTURA DO CSIRT.CV

Artigo 4º

Funções

O CSIRT.CV possui as seguintes funções:

a) Exercer a coordenação operacional na resposta a incidentes, nomeadamente em articulação com as equipas de resposta a incidentes de segurança informática setoriais existentes ou a serem designadas para o efeito;

b) Monitorizar os incidentes com implicações a nível nacional e internacional;

c) Ativar mecanismos de alerta rápido;

d) Intervir na reação, análise, mitigação de incidentes e resolução, por uma equipa multidisciplinar visando a reposição do estado normal de funcionamento;

e) Proceder à análise dinâmica dos riscos;

f) Participar nos e assegurar a representação nacional nos *foruns* de cooperação de equipas de resposta a incidentes de segurança de informação;

g) Participar em eventos de treino nacionais e internacionais;

h) Receber, armazenar e indexação de dados (eventos) dos principais sistemas das infraestruturas críticas do Estado e Fornecedores de Internet;

i) Transformação e correlação de dados de modo a obter informações úteis em termos de cibersegurança da organização a partir de eventos de tecnologias diferentes;

j) Alertas para o todo o pessoal relevante em caso de ocorrência de incidentes através de sistemas autónomos e da equipa de monitorização e análise;

k) Análise de incidentes (anomalias), em tempo real, através da equipa de monitorização e análise, visando a descoberta de todas as informações relevantes para a mitigação e resolução;

l) Investigação profunda (forense) e posterior produção do respetivo relatório de incidente detalhando os acontecimentos, as causas, as consequências e eventuais medidas a serem tomadas para prevenir uma nova ocorrência;

m) Comunicação com outros CSIRT (Computer Security Incident Response Team) a nível mundial e formação do pessoal relevante para o aspeto da cibersegurança;

n) Receber e tratar alertas da população em geral referente a falhas e ameaças detetadas por utilizadores comuns.

Artigo 5º

Local de funcionamento

1- O CSIRT.CV deve ser localizado num espaço físico onde possa partilhar as condições de segurança física e equipamentos de suporte já existentes, nomeadamente nas instalações do *Data Center* do Estado, sem prejuízo da obrigatoriedade de gestão técnica autónoma.

2- O previsto no número anterior não impede que venha a ser instalado em sede própria, garantindo-se os mesmos níveis de segurança física e equipamentos de suporte exigidos pelas funções a desempenhar.

Artigo 6º

Recursos Humanos

1- O CSIRT.CV é composto por equipas com diferentes competências e qualificações, para os três níveis correspondentes a diferentes responsabilidades:

a) Nível I: equipa de monitorização e análise, responsável pela monitorização e análise constante dos eventos, alertando, caso se verifique um incidente, a equipa de nível II;

b) Nível II: equipa de resposta a incidentes, composta por especialistas que se encarregam da resolução de problemas reportados pela equipa de Nível I;

c) Nível III: equipa de investigação (forense), que investiga áreas relevantes na matéria de cibersegurança, cria procedimentos para incidentes, propõe medidas preventivas, garante a comunicação com outros CSIRT (*Computer Security Incident Response Team*), fornece informações ao pessoal dos demais níveis, bem como outras Entidades que devam ter acesso a essa informação, nomeadamente as autoridades judiciárias e órgãos de polícia criminal.

2- O perfil e competências do pessoal do CSIRT.CV é aprovado em diploma próprio, que estabelece o seu plano de carreiras, cargos e salários.

Artigo 7º

Equipa de Nível I

1. No nível I, a equipa deve garantir a monitorização e a triagem dos eventos de forma ininterrupta, 24h por dia e 7 dias por semana.

2. A equipa tem formação básica para poder analisar os dados fornecidos pelo SIEM, seguir procedimentos para resolução de problemas simples e entender conceitos básicos de cibersegurança.

3. Devido ao caráter ininterrupto do trabalho, a equipa deve ser composta por um número mínimo de 3 pessoas, mantendo sempre um regime de piquete organizado por turnos.

Artigo 8º

Responsabilidades

A equipa do nível I deve assumir as seguintes responsabilidades:

a) Monitorizar e analisar continuamente os eventos, nomeadamente as informações fornecidas pelo SIEM;

b) Fazer a triagem dos eventos, categorizando-os por natureza e determinando a relevância e urgência de eventuais incidentes;

c) Sinalizar um incidente, dar o alerta;

d) Seguir os procedimentos definidos para incidentes;

e) Receber e dar seguimento a alertas comunicadas por outros *CSIRTS/CSIRTs* ou pelo público;

f) Elaborar relatórios preliminares.

Artigo 9º

Equipa de Nível II

1- No nível II, a equipa de resposta a incidentes é multidisciplinar, sendo constituída por especialistas em diferentes tecnologias utilizadas pela organização.

2- A função da equipa de resposta a incidentes é fazer a mitigação e resolução do incidente, executando, designadamente, as seguintes tarefas:

a) Caracterizar e analisar o tráfego na rede de dados de forma a identificar atividade anómala e potenciais ameaças aos recursos de rede e à Informação;

b) Coordenar com os elementos que contribuem para a segurança da rede de dados, de forma a validar alertas relacionados com a rede;

c) Monitorizar fontes de informação de segurança como os portais de fabricantes de produtos de segurança, sistemas operativos, antivírus, equipas de Resposta a Incidentes Informáticos de outras organizações, para manter atualizada a informação sobre ameaças e determinar com colaboração do *Vulnerability Manager*/*Pentester* quais os casos que podem ter impacto nos Sistemas de Informação instalados na rede de dados do Estado de Cabo Verde;

d) Documentar e escalar incidentes que possam vir a ter um impacto mais alargado nas redes ou sistemas;

e) Efetuar relatórios de análise de tendências relativas à segurança da rede;

f) Efetuar correlação de eventos, utilizando informação obtida de diversos sensores da rede para obter conhecimento situacional da rede de dados e determinar a eficácia dos ataques detetados;

g) Providenciar relatórios diários sobre eventos de segurança relevantes para a defesa da rede e Sistemas de Informação;

h) Receber e analisar alertas de segurança de várias fontes da rede de dados e determinar as causas possíveis;

i) Detetar, identificar e alertar atempadamente para possíveis ataques, intrusões, atividades anómalas ou má conduta por parte dos utilizadores, de forma a distinguir incidentes e eventos de atividades normais;

j) Utilizar ferramentas para monitorizar e analisar a rede de dados de forma a identificar atividade maliciosa;

k) Analisar atividades maliciosas que tenham sido identificadas para identificar as vulnerabilidades exploradas e os efeitos nos Sistemas de Informação;

l) Efetuar o controlo de qualidade do código de todas as aplicações desenvolvidas pelas organizações ou adquiridas a entidades terceiras, parceiros, stakeholders, com base em *frameworks* como OWASP ou ISO/IEC 25000:2014 (norma de qualidade de software);

m) Utilizar práticas e princípios de defesa em profundidade apoiadas por meios SIEM;

n) Determinar as ações apropriadas de forma a responder às atividades anómalas analisadas;

o) Efetuar testes aos controlos de segurança da Garantia de Informação, de acordo com os planos e procedimentos em vigor;

p) Determinar Táticas, Técnicas e Procedimentos para fazer face a diferentes tipos de incidentes;

q) Recomendar correções de vulnerabilidades a computadores, redes e sistemas;

r) Identificar e analisar anomalias recorrendo a metadados;

s) Examinar a topologia da rede de forma a perceber o fluxo de dados na rede de dados;

t) Validar alertas de sistema de deteção de intrusões com o tráfego analisado através de ferramentas de análise pacotes e protocolos;

u) Efetuar pesquisa, análise e correlação de eventos recorrendo às diversas fontes;

v) Identificar aplicações e sistemas operativos de dispositivos na rede de dados, de acordo com o tráfego detetado na rede;

w) Analisar as políticas e configurações da rede de dados e avaliar a conformidade com regulamentações e diretivas do Estado de Cabo Verde;

x) Conduzir e/ou apoiar testes de análise de vulnerabilidades ou de penetração que estejam autorizados aos meios da rede de dados;

y) Adquirir aplicações e *hardware* necessários à condução de análise de vulnerabilidades e testes de penetração;

z) Estar atualizado quanto às vulnerabilidades mais recentes, bem como a todo o *software* usado na rede de dados;

aa) Manter um conjunto de aplicações e equipamentos preparados para efetuar trabalhos de auditoria em qualquer parte da rede de dados;

bb) Testar novas vulnerabilidades em coordenação com o *Network Security Engineer*;

cc) Manter conhecimento atualizado de políticas de proteção da rede de dados, regulamentos e documentos de conformidade que estejam relacionados com as auditorias à rede de dados;

dd) Preparar relatórios de auditoria que salientem o que for identificado ao nível de procedimentos e situações técnicas, de forma a recomendar soluções ou estratégias de mitigação ou remediação;

ee) Realizar análises de risco e de vulnerabilidades à tecnologia, pessoas e modo de operação em locais importantes como gabinetes, infraestrutura de suporte e a rede de dados;

ff) Apoiar na escolha e se seleção de controlos de segurança que apresentem uma boa relação custo / benefício de forma a mitigar o risco e proteger a informação, processos e sistemas.

Artigo 10º

Responsabilidades

Os elementos da equipa do Nível II deve assumir as seguintes responsabilidades:

a) Análise suplementar do incidente;

b) Mitigação e resolução do problema;

c) Produção de relatórios de incidentes e recomendações.

Artigo 11º

Equipa de Nível III

1- No Nível III, a equipa de cibersegurança garante a gestão do CSIRT e atua de forma preventiva analisando incidentes, identificando eventuais vulnerabilidades e propondo medidas de prevenção.

2- A cooperação com outros CSIRT a nível global para partilha de informações e assistência, ficam a cargo da equipa de cibersegurança.

Artigo 12º

Responsabilidades

Os elementos da equipa do nível III deve assumir as seguintes responsabilidades:

a) Propor a criação e atualização de procedimentos para diferentes tipos de incidentes;

b) Propor a criação de políticas de segurança de informação para as infraestruturas críticas;

c) Proceder a auditoria de Segurança de Informação nas infraestruturas críticas;

d) Gerir o processo de resposta a incidentes e do CSIRT;

e) Proceder à investigação (forense) de incidentes e proposta de medidas preventivas;

f) Proceder à análise de eventuais vulnerabilidades nos sistemas das instituições sobre as quais o CSIRT tenha ação;

g) Executar ações de *pentest as a service* de forma a garantir uma contínua proatividade sobre o estado da segurança dentro e fora da rede de dados. Integrar com conectores específicos com o SIEM de forma a dar visibilidade das vulnerabilidades internas e externas dos serviços publicados pelos IPs públicos e privados de todas as organizações);

h) Comunicar com outros CSIRT *(Computer Security Incident Response Team);*

i) Formar pessoal relevante em matérias de cibersegurança;

j) Produzir relatórios periódicos relativo ao CSIRT com informação tratada sobre número e tipos de incidentes ao longo desse período, bem como recomendações aos *stakeholders;*

k) Extrair indicadores por meio da combinação de artefactos digitais, análise de código e reverse e*ngineering*, execução de *malware* em *runtime* e técnicas de simulação em ambiente laboratorial;

l) Manter *cyber threat intelligence* e aquisição de informação de várias fontes específicas selecionadas;

m) Detetar o local externo de origem com base em assinaturas, técnicas e análises específicas, destinadas a detetar e seguir e mitigar os APT;

n) Participar ativamente em grupos de partilha de *cyber threat intelligence*, normalmente compostos por outros SOC, CSIRTs, organizações e indústrias, com suporte semelhante;

o) Analisar de forma avançada incidentes e suporte a respostas de segurança, tais como análise forense de imagens obtidas a partir da memória e discos rígidos;

p) Proceder à criação e *tunning* de análises avançadas para detetar modelos de ataque complexos ou avançados, como os utilizados para detetar e seguir os APT'S através de ferramenta própria de *Managed Security Systems;*

q) Desenvolver ferramentas personalizadas orientadas para detetar, monitorizar, manter (para efeitos de investigação) ou bloquear os APT'S em diferentes fases do ciclo dos ciberataques;

r) Exercer e completar uma capacidade de gestão do conhecimento das ameaças, permitindo que os analistas do CSIRT interliguem atividades, incidentes, indicadores e diferentes artefactos;

s) Acompanhar tendências e elaborar relatórios de atividade e incidentes relacionados com os APT'S;

t) Investigar a presença de APT´s nas redes monitorizadas pelo CSIRT;

u) Proceder a *Honeypotting* e outros métodos de recolha que permitem à equipa coletar, analisar, investigar e monitorizar novas ameaças;

v) Permitir o fornecimento de serviços mais simples e rápido, através da redução da dependência de terceiros que processam *malware* e análise forense.

CAPÍTULO III

PROCEDIMENTOS

Artigo 13º

Procedimentos

1- Os procedimentos das equipas do CSIRT.CV são padronizados, visando uma maior coordenação e uma utilização eficiente dos recursos.

2- Os procedimentos constam de regulamento, aplicável ao pessoal do CSIRT.CV, bem como os todas entidades e instituições previstas no artigo 2º do presente diploma.

3- O Regulamento de procedimentos do CSIRT.CV é aprovado por Portaria Conjunta dos membros do Governo responsáveis pelas áreas da administração interna e da economia digital, mediante Parecer da Comissão Nacional de Proteção de Dados.

Artigo 14º

Monitorização

1- A monitorização realizada pela equipa de monitorização e análise é feita continuamente, 24h por dia e 7 dias por semana.

2- Os dados para o processo de monitorização devem ser fornecidos pelo SIEM que recebe, armazena, correlaciona e transforma eventos recebidos dos equipamentos em informações que permitam monitorizar o Estado em termos de cibersegurança.

3- O SIEM deve apresentar informações em formatos amigáveis, como por exemplo gráfico ou quadros, e detetar anomalias, notificando a equipa de monitorização e análise.

4- Os dados a serem monitorizados e a forma de monitorização são especificados para cada tipo de equipamento através de procedimentos definidos pela equipa de cibersegurança.

Artigo 15º

Deteção, Análise e escalonamento

1. A equipa de monitorização e análise é responsável pelos processos de deteção, análise e escalonamento, necessitando de uma hierarquia na equipa para tomada de decisões.

2. Qualquer violação ou ameaça eminente das políticas de segurança, políticas de utilização ou práticas de segurança, incluindo eventos como obtenção de dados de forma não autorizada, acessos a sistemas não autorizados, comprometimento de sistemas ou atividades de *malwares*, é categorizada como um incidente.

3. Os dados a serem analisados e a forma de análise, de maneira a obter informações que auxiliem na resolução e investigação do incidente, são especificados de acordo com o tipo de incidente e equipamento em procedimentos definidos pela equipa de cibersegurança.

4. A equipa de monitorização e análise decide o escalonamento de acordo com a análise feita, fazendo uso do IMS para coordenar o processo de resposta e alertar o pessoal relevante.

Artigo 16º

Mitigação e Resolução

1- A equipa de resposta a incidentes assume a responsabilidade da mitigação e resolução do problema após de ser notificada, com recurso ao IMS.

2- A equipa de cibersegurança também pode fazer parte do processo de mitigação e resolução, cooperando com a equipa de resposta a incidentes.

3- Os procedimentos a serem seguidos para mitigação e resolução de incidentes são determinados por um conjunto de procedimentos para tipos de incidentes e equipamentos específicos, que são elaborados pela equipa de cibersegurança.

4- É estabelecida uma ordem hierárquica clara, que permita e a tomada de decisões em relação a aspetos não determinados pelos procedimentos.

5- As ações realizadas são documentadas e partilhadas com o pessoal competente na matéria, fazendo-se uso do IMS para coordenar e acompanhar todo o processo de resposta aos incidentes.

Artigo 17º

Investigação forense e prevenção

1- A equipa de cibersegurança deve fazer uma investigação forense profunda dos incidentes, com vista a analisar detalhadamente os incidentes.

2- É produzido um relatório de incidentes que especifique as causas, as consequências, as medidas tomadas e o resultado das mesmas.

3- A equipa de cibersegurança deve, caso seja necessário, propor medidas para evitar que um incidente se repita.

4- Caso se justifique, a equipa de cibersegurança pode fazer uma verificação de vulnerabilidades e monitorização com vista a determinar ações adicionais necessárias.

5- Caso seja necessário, a equipa de cibersegurança deve criar ou rever procedimentos para resolução de incidentes.

6- Novas formas de monitorização podem ser adicionadas ao SIEM pela equipa de cibersegurança, como forma de prevenir que um incidente ocorra novamente.

CAPÍTULO IV

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Artigo 18º

Política de Segurança da Informação

1- As atividades do CSIRT.CV cumprem as normas previstas pelo decreto-lei n.º 19/2010, de 14 de junho, que designa o Núcleo Operacional da Sociedade de Informação (NOSi) como responsável pela gestão da Rede Tecnológica Privativa do Estado (RTPE), tendo como obrigação garantir a segurança e operacionalidade da RTPE e implementar o processo de segurança da informação, estando autorizado a monitorizar os acessos através de registo e atividades de segurança da informação.

2- O CSIRT.CV deve garantir que os dados sob a sua custódia, estejam protegidos de forma a evitar o uso ou o acesso não autorizado dos sistemas de informações, manter a integridade, disponibilidade e privacidade das informações confidenciais e evitar perda ou destruição.

3- Deve ser assegurada a privacidade individual, garantindo que os dados pessoais não são divulgados, utilizados de forma imprópria, nem disponibilizados a terceiros, exceto nas situações previstas na lei e no estrito cumprimento do regime jurídico de proteção de dados pessoais.

4- O CSIRT.CV respeita a estrutura organizacional definida no artigo 6º, devendo ser composto por 3 (três) equipas com diferentes responsabilidades, tal como previsto no presente diploma.

5- Sem prejuízo das normas legais aplicáveis, o perfil para recrutamento e a formação/qualificação do pessoal, devem obedecer os requisitos e competências previstos no Capítulo II do presente diploma.

6- A infraestrutura deve possuir um SIEM, um IMS e um espaço físico com as caraterísticas especificadas no presente diploma.

Artigo 19º

Natureza administrativa

1- O CSIRT.CV é uma estrutura de missão dotado de autonomia administrativa, financeira e patrimonial.

2- O CSIRT.CV é gerido por uma comissão, nomeada por Resolução do Conselho de Ministros, cujos integrantes são escolhidos de entre as entidades que integram o Núcleo Nacional de Cibersegurança, previsto pelo artigo 4º da Resolução n.º 21/2016, de 7 de março, que aprovou a Estratégia Nacional de Cibersegurança, que funciona provisoriamente na dependência direta do Primeiro Ministro, até à sua instalação e enquadramento definitivos.

3- A Resolução que nomeia os integrantes da Comissão de gestão define também os seus objetivos específicos e competências.

4- A Comissão a que se refere o número anterior é extinta com a transferência do CSIRT.CV para a estrutura do Centro Nacional de Cibersegurança, através do diploma de instalação deste.

Artigo 20º

Entrada em vigor

O presente diploma entra em vigor no dia seguinte ao da sua publicação.

Aprovado em Conselho de Ministros, aos 17 de dezembro de 2020. — Os Ministros, *José Ulisses de Pina Correia e Silva, Olavo Avelino Garcia Correia* e *Paulo Augusto Rocha.*

Promulgado em 27 de janeiro de 2021

Publique-se.

O Presidente da República, JORGE CARLOS DE ALMEIDA FONSECA.

I SÉRIE
BOLETIM OFICIAL

Registo legal, nº 2/2001, de 21 de Dezembro de 2001

Endereço Electronico: *www.incv.cv*

IMPRENSA NACIONAL DE CABO VERDE

Av. da Macaronésia,cidade da Praia - Achada Grande Frente, República Cabo Verde
C.P. 113 • Tel. (238) 612145, 4150 • Fax 61 42 09
Email: kioske.incv@incv.cv / incv@incv.cv

I.N.C.V., S.A. informa que a transmissão de actos sujeitos a publicação na I e II Série do *Boletim Oficial* devem obedecer as normas constantes no artigo 28º e 29º do Decreto-lei nº 8/2011, de 31 de Janeiro.