Política regional de proteção das infraestruturas essenciais da CEDEAO

PARTE 1. INTRODUÇÃO

Em todos os países há um certo número de serviços materiais ou imateriais fornecidos pelos operadores públicos ou privados que são essenciais para a Nação e, em particular, para o funcionamento do Estado, da economia, saúde, segurança e bem-estar da população. Estes serviços assentam sobre um conjunto de infraestruturas físicas ou digitais, assim como sobre os dados necessários ao seu funcionamento.

Por isso, é extremamente importante para o Estado, para os operadores económicos e para a população assegurar a resiliência e a segurança destas infraestruturas críticas, serviços essenciais e dados, perante todos os riscos e ameaças que poderão afetar a sua disponibilidade e integridade.

Com efeito, a resiliência e a segurança das infraestruturas críticas e serviços essenciais podem ser afetadas por diversos riscos e ameaças - avarias, acidentes, atos criminosos, agressões físicas, ataques informáticos, catástrofes naturais, pandemias, etc. -, os quais podem ter um grave impacto sobre a Nação. Então, é importante que a proteção de cada infraestrutura crítica ou serviço essencial tenha em conta todos estes tipos de riscos e ameaças físicas e informáticas.

Além disso, certos serviços podem estar baseados sobre infraestruturas e dados situados no estrangeiro. Neste caso, a proteção destes serviços não pode ser totalmente assegurada pelo país que os fornece. Isto justifica o facto de cada Estado integrar no seu programa os serviços essenciais que lhe são necessários assim como as infraestruturas críticas situadas no seu território. Este tipo de situação justifica também a abordagem regional da presente política.

Neste documento, os dados serão considerados como fazendo parte das infraestruturas que os armazenam, tratam ou transmitem.

PARTE 2. ASSUNTO

A presente política regional tem por objetivo assegurar a resiliência e a segurança perante os diversos riscos e ameaças que poderão afetar o funcionamento das infraestruturas e serviços da região que são essenciais para o funcionamento do Estado, para a economia, saúde, segurança e bem-estar da população, nomeadamente quando estes serviços e infraestruturas têm um carácter transnacional.

Com essa finalidade, esta política regional:

- fixa o quadro normativo mínimo que os Estados-Membros deverão adotar para assegurar a proteção das suas infraestruturas críticas e serviços essenciais;
- apresenta os elementos de metodologia e os critérios que devem ser utilizados para a identificação das infraestruturas e serviços nos vários setores de atividade;
- propõe uma lista de medidas preventivas, reativas e proativas que podem ser aplicadas;
- prevê os princípios e modalidades de cooperação entre os Estados-Membros que têm uma interdependência em matéria de serviço essencial ou de infraestrutura crítica.

A presente política regional não deve prejudicar a possibilidade que cada Estado tem de adotar as medidas necessárias para assegurar a proteção dos seus interesses essenciais e a sua segurança, assegurar a ação e a segurança públicas e permitir a pesquisa, deteção e punição de infrações penais.

PARTE 3. DEFINIÇÕES

No âmbito desta política regional, entende-se por:

Cibersegurança: o conjunto das medidas e ações destinadas a proteger o ciberespaço e os meios informáticos das ameaças que estão associadas ou que podem prejudicar a sua rede e infraestrutura de informação. A cibersegurança visa preservar a disponibilidade e a integridade das redes e da infraestrutura assim como a confidencialidade das informações;

Cibercriminalidade: as atividades criminais que visam os computadores e os sistemas informáticos quer como ferramenta primária, quer como alvo principal. A cibercriminalidade abrange os delitos habituais (fraude,

contrafação e usurpação de identidade, por exemplo), os delitos relativos ao conteúdo (distribuição em linha de material pedo pornográfico ou incitação ao ódio racial, por exemplo) e os delitos especificamente relacionados com os computadores e os sistemas informáticos (ataque contra um sistema informático, recusa de serviço e programa com vírus, por exemplo);

Infraestrutura crítica: uma infraestrutura ou um processo público ou privado cuja destruição, interrupção, exploração ilegítima ou perturbação durante um determinado período de tempo possa provocar a perda de vidas, prejuízos graves para a economia ou para a reputação do Estado ou dos seus símbolos. Nesta definição, a infraestrutura inclui as redes, os sistemas e os dados físicos ou virtuais indispensáveis ao funcionamento deste serviço. Esta expressão pode fazer referência a um sistema ou processo cujo funcionamento é crítico no âmbito da organização;

Infraestrutura crítica de informação: rede de comunicação ou sistema de informação cuja disfunção ou uma exploração maliciosa poderá provocar uma interrupção total ou parcial de uma infraestrutura crítica ou de um serviço essencial;

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

Proteção das infraestruturas críticas: conjunto das medidas e ações destinadas a proteger as infraestruturas críticas contra todos os riscos e ameaças suscetíveis de provocar a interrupção total ou parcial dos serviços essenciais que fornecem;

Proteção das infraestruturas críticas da informação: cibersegurança das infraestruturas críticas, isto é, o conjunto das medidas e ações destinadas a proteger as redes de comunicação e os sistemas de informação contra as ameaças cibernéticas, cuja perturbação ou paragem poderia provocar interrupção total ou parcial de uma infraestrutura crítica ou de um serviço essencial;

CSIRT (Computer Security Incident Response Team/Equipa de Resposta a Incidentes de Segurança Informática): equipa responsável por alertar sobre ameaças, prevenir riscos e ameaças aos sistemas de informação, reagir a incidentes de segurança e ajudar na mitigação.

Serviço essencial: um serviço cuja interrupção total ou parcial poderia ter um impacto grave no funcionamento do Estado, na economia do país, saúde, segurança e bem-estar da população ou uma combinação de impactos deste tipo que individualmente não seriam suficientes para classificar o serviço como essencial;

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

Proteção de serviços essenciais: conjunto das medidas e ações destinadas a proteger os serviços essenciais de todos os riscos e ameaças suscetíveis de provocar a sua interrupção total ou parcial;

Tecnologias da informação e da comunicação (TIC) : tecnologias utilizadas para coletar, armazenar, tratar e transmitir informações incluindo as tecnologias que implicam a utilização de computadores ou de qualquer sistema de comunicação ou de telecomunicação.

Sistema de informação: qualquer dispositivo, isolado ou não, ou o conjunto de dispositivos interligados capazes de garantir, total ou parcialmente, o tratamento automatizado dos dados em execução de um programa;

Redes: conjunto dos meios que asseguram a alimentação de uma infraestrutura com os produtos ou serviços necessários ao seu funcionamento (comunicações, energia, logística, etc.);

CSIRT (*Computer Security Incident Response Team*) : equipa responsável por alertar sobre ameaças, prevenir os riscos relacionados com os sistemas de informação, reagir em caso de incidentes de segurança e ajudar a atenuar os seus efeitos.

PARTE 4. QUADRO DE PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICAS E DOS SERVIÇOS ESSENCIAIS

Cada Estado deverá adotar um quadro de proteção das infraestruturas críticas e dos serviços essenciais para todos os setores de atividade (atividades do Estado, saúde, energia, transportes, água, banca, indústria, etc.) e, em particular, os setores transversais (produção e distribuição de eletricidade e serviços digitais), estabelecendo:

- as responsabilidades no âmbito do Estado;
- os critérios e as modalidades de identificação das infraestruturas críticas e dos serviços essenciais;
- as modalidades de designação dos operadores de serviços essenciais e das infraestruturas críticas;
- as obrigações de segurança destes operadores.

Cada Estado deverá identificar, para os diferentes setores de atividade, a/as autoridade/s encarregada/s de:

- identificar os serviços essenciais e as infraestruturas críticas;
- designar os operadores correspondentes;
- elaborar as medidas de segurança que lhes serão impostas;
- assegurar a coordenação da ação das autoridades públicas que devem contribuir para a segurança das infraestruturas críticas e dos serviços essenciais;
- participar na gestão de crise em caso de incidentes graves que afetem uma infraestrutura crítica;
- assegurar a coordenação destas diferentes tarefas com o(s) seu(s) homólogo(s) estrangeiro(s) no caso das infraestruturas críticas transnacionais.

Cada Estado deverá criar uma estrutura responsável por assegurar a coerência das estratégias estabelecidas pelas várias autoridades nacionais.

PARTE 5. PAPÉIS RESPETIVOS DO ESTADO E DOS OPERADORES

Os operadores das infraestruturas críticas e dos serviços essenciais são responsáveis pela sua proteção. No entanto, o Estado, garante da segurança da Nação, tem a responsabilidade de garantir a segurança das infraestruturas críticas e dos serviços essenciais do país. Deve, em particular, identificar e designar os operadores dos serviços essenciais e das infraestruturas críticas, fixar-lhes obrigações de proteção, controlar o cumprimento das mesmas e sancionar as eventuais infrações.

Além disso, a proteção das infraestruturas críticas e dos serviços essenciais não pode ser assegurada apenas pelos operadores em questão, uma vez que estes não têm legitimidade nem geralmente os conhecimentos e as informações pertinentes para intervirem fora da sua área de responsabilidade. O Estado deve desempenhar o seu papel fornecendo aos operadores instruções e apoio numa estreita parceria público-privada. Deverá, em particular, intervir na prevenção das ameaças e na gestão de situações em caso de ataque físico ou cibernético, nomeadamente através das suas autoridades, serviços de informação, forças de ordem, CSIRT nacionais e instituições judiciais.

PARTE 6. ESTRATÉGIA DE GESTÃO DOS RISCOS

A proteção das infraestruturas críticas e dos serviços essenciais constitui um fardo pesado a nível organizacional, técnico, humano e financeiro. Por isso, é conveniente assegurar a proteção reforçada apenas das infraestruturas e serviços realmente críticos ou essenciais, e naquilo que é necessário.

Nesta perspetiva, deverá ser implementada uma estratégia de gestão dos riscos como aplicação da presente política, a fim de se identificarem os riscos e as ameaças potenciais e de se adequarem os esforços à probabilidade de ocorrência e à gravidade para a Nação.

Esta estratégia permitirá nomeadamente a cada Estado:

- identificar e designar as infraestruturas críticas, os serviços essenciais e os operadores públicos e privados adequados;

- definir, de acordo com a necessidade, as medidas destinadas a proteger estas infraestruturas e serviços face aos riscos e ameaças físicas e cibernéticas suscetíveis de terem um impacto grave na Nação, bem como as medidas para minimizar os impactos potenciais.

PARTE 7. IDENTIFICAÇÃO DAS INFRAESTRUTURAS CRÍTICAS E DOS SERVIÇOS ESSENCIAIS E DESIGNAÇÃO DOS OPERADORES

O processo deve começar pela identificação dos serviços essenciais e, em seguida, das infraestruturas necessárias para o fornecimento desses serviços ou que são críticas por outras razões. No Anexo I apresenta-se, por setor de atividade, uma lista não exaustiva de infraestruturas e serviços suscetíveis de serem classificados como críticos ou essenciais.

O processo deve continuar com a identificação dos operadores das infraestruturas críticas ou dos serviços essenciais. No Anexo II são propostos alguns critérios padrão. Em seguida, estes operadores devem ser sujeitos a um procedimento formal de aprovação e de designação.

PARTE 8. OBRIGAÇÕES DOS OPERADORES

No Anexo III é proposta uma lista não exaustiva de medidas que podem ser impostas aos operadores das infraestruturas críticas e dos serviços essenciais.

Estes operadores devem ser obrigados no mínimo a:

- criar uma estrutura a nível da direção para organizar e proteger as suas instalações;
- respeitar as regras técnicas e operacionais destinadas a melhorar a segurança física e cibernética das suas instalações;
- declarar rapidamente às autoridades competentes qualquer incidente suscetível de ter um impacto grave;
- colaborar sinceramente e sem reservas com as autoridades em caso de necessidade.

Qualquer operador de infraestruturas críticas ou de serviços essenciais deve criar e respeitar as medidas de proteção que lhe são impostas. Deve descrevê-las nos seguintes documentos que devem ser apresentados às autoridades competentes para a gestão da cibersegurança em cada Estado-Membro:

- um organograma dos seus serviços essenciais;
- um plano de segurança do operador;
- uma política de segurança dos sistemas de informação (PSSI) no que diz respeito à cibersegurança evidenciando os sistemas de informação mais críticos para os serviços essenciais que fornece.

PARTE 9. MEDIDAS DE PROTEÇÃO

Uma análise do risco, baseada em cenários que tenham em conta os vários riscos e ameaças identificados, deve permitir elaborar medidas de proteção para cada operador ou tipo de operador de infraestruturas críticas ou serviços essenciais.

Estas medidas são preventivas, reativas e proativas e podem também ser organizacionais, operacionais, técnicas ou jurídicas.

As medidas preventivas devem ter por objetivo prevenir e atenuar os riscos e ameaças, e ainda reduzir, tanto quanto possível, a gravidade dos impactos potenciais sobre a infraestrutura ou serviço em questão e sobre a Nação. As medidas reativas devem ser planeadas e implementadas em caso de incidente que afete a infraestrutura crítica ou o serviço essencial. Devem permitir assegurar a gestão do incidente, até ao reinício normal da atividade, e a gestão da crise que este incidente possa provocar na Nação. As medidas proativas visam evitar a recorrência de incidentes examinando as possíveis causas dos incidentes ocorridos e adotando uma estratégia que permita detetar e conter qualquer incidente idêntico. Apenas devem ser tomadas medidas realistas que possam ter um efeito concreto sobre os objetivos acima referidos.

As medidas destinadas a proteger as infraestruturas e os serviços críticos contra riscos e ameaças que utilizem ou afetem as tecnologias da informação e da comunicação devem ser coerentes com a Estratégia Regional de Segurança Cibernética e Combate à Cibercriminalidade.

Além disso, os Estados-Membros devem ter em conta na sua política nacional as medidas de proteção já previstas nos regulamentos internacionais para todos os setores-chave (transporte aéreo, navegação marítima, transações bancárias, etc.).

PARTE 10. SANÇÕES PENAIS

Devem ser previstas sanções, incluindo sanções penais e administrativas, quando forem necessários, contra os operadores e outras partes que não respeitam as medidas de proteção.

Além disso, o direito penal deverá impor penas (penais e administrativas) mais severas para infrações por operadores e outras partes que tenham perturbado ou tentado perturbar o bom funcionamento das infraestruturas críticas e dos serviços essenciais.

PARTE 11. INTERDEPENDÊNCIAS DAS INFRAESTRUTURAS CRÍTICAS E SERVIÇOS ESSENCIAIS

O processo deve ter em conta as interdependências que possam existir entre as infraestruturas críticas e os serviços essenciais. Por exemplo, todos os serviços e infraestruturas são, salvo raras exceções, dependentes dos serviços de distribuição elétrica e de comunicações eletrónicas.

Por conseguinte, cada Estado deverá criar meios alternativos[1] para evitar qualquer interrupção no funcionamento das infraestruturas críticas e dos serviços essenciais que possam ter um impacto grave na Nação.

PARTE 12. COORDENAÇÃO NACIONAL

Cada Estado deverá mobilizar todas as autoridades e entidades públicas em questão, incluindo nomeadamente a estrutura responsável pela segurança cibernética a nível nacional, para estabelecer uma política nacional de proteção das infraestruturas críticas e dos serviços essenciais e fixar a contribuição de cada um para a sua implementação, tanto em relação às medidas preventivas como às reativas.

As autoridades e os parceiros públicos devem estabelecer um diálogo com os operadores das infraestruturas críticas e dos serviços essenciais para identificar com cada um deles as suas principais vulnerabilidades, as medidas adequadas para as reduzir e os prazos razoáveis para a implementação destas medidas.

PARTE 13. INTERDEPENDÊNCIAS ENTRE OS PAÍSES DA REGIÃO E COOPERAÇÃO REGIONAL

As interdependências entre países continuam a aumentar na CEDEAO e na Mauritânia, nomeadamente no que respeita aos serviços essenciais.

Para além dos serviços interligados que, pela sua natureza, dizem respeito a todos os países, como as telecomunicações públicas, as transações financeiras ou os transportes aéreos internacionais, existem cada vez mais infraestruturas que servem vários países, como por exemplo nas áreas dos corredores rodoviários, conexão global à Internet, eletricidade, minas, gás e Sistema de Informação da Polícia da África Ocidental (SIPAO), em vigor em todos os Estados-membros da CEDEAO e na Mauritânia.

Certos serviços podem ser designados como serviços essenciais por todos os Estados-Membros envolvidos. Outros, sendo essenciais num determinado país, podem depender de infraestruturas situadas num outro país que não as identifique como críticas.

[1] Instalação de geradores elétricos ou de alternativas às ligações elétricas ou eletrónicas, por exemplo.

Face a esta dupla problemática, é conveniente incentivar o diálogo e a cooperação entre os Estados-Membros da região, com base numa compreensão comum das questões e em disposições com um nível adequado de proteção e tão semelhantes e suficientes quanto possível em todos os países.

Os Estados-Membros com serviços essenciais ou infraestruturas críticas interdependentes são, assim, convidados a estabelecer uma cooperação entre as suas autoridades competentes com vista a:

- Identificar os serviços essenciais e as infraestruturas críticas de carácter transnacional assim como a natureza das suas interdependências;
- Ter em conta, tanto quanto possível, as necessidades dos outros Estados-Membros na designação das suas infraestruturas críticas;
- Harmonizar as medidas de proteção impostas aos operadores em questão;
- Trocar informações sobre ameaças e riscos e tomar eventuais medidas complementares necessárias de forma coordenada para responder a uma ameaça ou risco crescente ou iminente;
- Coordenar as medidas a tomar em caso de crise relacionada com uma infraestrutura crítica transnacional.

PARTE 14. ACOMPANHAMENTO E ATUALIZAÇÃO DA PRESENTE POLÍTICA REGIONAL

A Comissão da CEDEAO criará um comité para acompanhar esta política. O comité de acompanhamento, composto pela Comissão da CEDEAO e por um representante de alto nível proposto por cada Estado-membro, reunir-se-á, pelo menos, uma vez por ano para garantir o cumprimento das disposições desta política regional no tempo previsto e propor as alterações que sejam necessárias.

ANEXO I

Infraestruturas e serviços que podem ser classificados como críticos ou essenciais

O processo de identificação dos operadores das infraestruturas críticas e dos serviços essenciais deve ter em conta a lista não exaustiva das infraestruturas e serviços apresentados no quadro seguinte:

Setores	Infraestruturas e serviços
1. Atividades do Estado	- Segurança pública - Segurança interna - Serviços judiciários - Defesa nacional - Finanças públicas - Parlamento - Processos eleitorais - Administração eletrónica, nomeadamente certos serviços públicos em linha
2. Energia	- Produção, transporte e distribuição elétrica - Produção, transporte, refinação, armazenamento e distribuição de produtos petrolíferos - Produção, transporte, tratamento, armazenamento e distribuição de gás - Instalações nucleares
3. Transporte	- Transporte aéreo, rodoviário, ferroviário, marítimo e fluvial - Controlo da circulação aérea - Gestão da plataforma aeroportuária e portuária (incluindo os sistemas de segurança) - Gestão da infraestrutura rodoviária e ferroviária
4. Logística	- Gestão das plataformas logísticas
5. Finanças	- Distribuição de mínimos sociais (intervenção de segurança/panfletos financeiros/incentivos sociais) - Distribuição dos mínimos sociais - Gestão da cobrança e da tesouraria dos organismos sociais - Transações bancárias - Serviços financeiros e de recuperação de crédito - Infraestruturas dos mercados financeiros
6. Saúde	- Capacidades ou procedimentos únicos de cuidados de saúde (nos estabelecimentos ou por telemedicina) - Distribuição farmacêutica - Laboratórios de pesquisa - Bases de dados de processos médicos
7. Água e saneamento	- Produção, transporte, armazenamento e distribuição de água potável (canalizada ou engarrafada) - Sistemas de recolha e de gestão de águas usadas
8. Comunicações eletrónicas	- Rede Internet nacional e ligação à Internet regional e mundial (cabos submarinos e terrestres, pontos de aterragem dos cabos, pontos de troca Internet, etc.) - Gestão dos nomes de domínio da Internet (DNS) - Fornecimento de acesso à Internet - Serviços de telecomunicações (telefone, etc.) - Centros de dados, incluindo, centros de Dados nacionais
9. Informação	- Rádio e televisão

10. Alimentação	- Fornecimento, armazenamento e distribuição dos principais produtos alimentares
11. Indústria	- Indústrias essenciais para o país
12. Diversos	- Infraestruturas suscetíveis de provocar prejuízos graves à população em caso de destruição acidental ou criminosa (barragem por exemplo)

ANEXO II

CRITÉRIOS DE IDENTIFICAÇÃO DOS OPERADORES DAS INFRAESTRUTURAS CRÍTICAS E DOS SERVIÇOS ESSENCIAIS

O processo de identificação dos operadores dos serviços essenciais e das infraestruturas críticas pode basear-se parcial ou totalmente nos critérios indicados na seguinte lista não exaustiva:

1. O nível de gravidade, a duração e a extensão do impacto que uma interrupção do serviço ou incidente teria no funcionamento do Estado, na economia ou na saúde, na segurança, proteção e bem-estar da população;
2. A dimensão da zona ou da população suscetível de ser afetada por um incidente;
3. O número de utilizadores que dependem do serviço (expresso em percentagem de população, por exemplo);
4. A quota de mercado do operador;
5. A dependência de outras infraestruturas críticas ou serviços essenciais deste serviço (como no caso dos serviços de distribuição da eletricidade e serviços de comunicações eletrónicas);
6. A importância do operador no que respeita à garantia de um nível de serviço adequado tendo em conta a disponibilidade de meios alternativos para o fornecimento do serviço;
7. Quando for apropriado, os fatores específicos do setor.

ANEXO III

MEDIDAS QUE PODEM SER IMPOSTAS AOS OPERADORES DAS INFRAESTRUTURAS CRÍTICAS E DOS SERVIÇOS ESSENCIAIS

Segue-se uma lista não exaustiva de medidas que podem ser impostas aos operadores das infraestruturas críticas e dos serviços essenciais.

Medidas preventivas

- Política de proteção:
    1. Designar uma autoridade responsável perante as autoridades públicas por todas as questões de segurança;
    2. Criar uma organização para garantir a proteção física e a segurança cibernética das infraestruturas do operador;
       Apresentar às autoridades públicas, segundo a periodicidade fixada por cada Estado, um relatório sobre os riscos, as ameaças, as vulnerabilidades identificadas e as principais medidas tomadas como resposta;

- Segurança física:
    1. Implementar uma estratégia de análise do risco para identificar e corrigir as principais vulnerabilidades que podem afetar gravemente a Nação;
    2. Sensibilizar e formar o pessoal;
    3. Garantir a segurança do acesso: gestão da identidade e dos direitos de acesso, dispositivos para proibir ou atrasar a entrada não autorizada, dispositivos de deteção de intrusos;
    4. Garantir a segurança face aos riscos naturais ou acidentais: dispositivos de prevenção e de luta contra incêndios, prevenção de inundações, prevenção de acidentes;
    5. Criar alternativas para as instalações ou fontes de alimentação mais críticas;
    6. Estabelecer e implementar um plano de segurança do operador (PSO);
    7. Possuir uma auditoria periódica de segurança física feita por um serviço estatal ou por um prestador de serviços aprovado pelo Estado, pelo menos de 5 em 5 anos;
    8. Estabelecer planos de continuidade e de reinício das atividades;
    9. Participar em formações e atividades com uma periodicidade determinada por cada Estado.

- Segurança cibernética:
    1. Implementar uma estratégia de análise do risco para identificar e corrigir as principais vulnerabilidades que possam ter graves consequências na Nação;
    2. Apresentar às autoridades uma cartografia das redes e sistemas de informação críticos e actualizá-la sempre que se verifiquem alterações significativas;
    3. Sensibilizar e formar o pessoal;
    4. Aplicar as regras de higiene informática;
    5. Manter os sistemas e as aplicações em boas condições de segurança;
    6. Fazer um mapa da cadeia de abastecimento e assegurar a sua higiene cibernética;
    7. Ter em conta os alertas dados pelo CSIRT;
    8. Garantir a segurança das redes e dos sistemas: regras sobre as configurações, partição, acesso remoto, filtragem;
    9. Garantir a segurança da administração das redes e dos sistemas: regras sobre as contas e os sistemas de administração;
    10. Garantir a segurança dos dados: fazer backup periódico, criar redundâncias e réplicas, encriptação dos dispositivos de armazenamento e dos canais de comunicação, etc.;

11. Assegurar a gestão das identidades e dos acessos: regras sobre a identificação, a autenticação, os direitos de acesso;
12. Garantir a defesa das redes e dos sistemas: deteção dos incidentes de segurança, registo de acontecimentos, correlação e análise dos registos;
13. Criar redundâncias para os sistemas ou fontes de alimentação mais críticas;
14. Criar e aplicar uma política de segurança dos sistemas da informação (PSSI);
15. Efetuar a homologação de segurança dos sistemas de informação críticos;
16. Mandar fazer uma auditoria de segurança dos sistemas de informação por um serviço estatal ou por um fornecedor de serviços aprovado pelo Estado, pelo menos de 3 em 3 anos e após cada incidente e alteração nos sistemas de informação;
17. Estabelecer planos de continuidade e reinício das atividades;
18. Participar em formações e atividades segundo uma periodicidade fixada por cada Estado;

Medidas reativas

1. Notificar imediatamente às autoridades públicas qualquer incidente que possa ter consequências graves;
2. Ativar mecanismos e sistemas para coletar e divulgar as informações pertinentes de forma atempada;
3. Ativar a organização interna de gestão de crises em coordenação com as autoridades públicas (responsáveis identificados e contatáveis, instalações, ligações, etc.);
4. Ativar os planos de continuidade e de reinício das atividades.

Medidas proactivas

1. Após o reinício das operações, analisar a causa do incidente;
2. Transmitir os resultados da análise às autoridades nacionais competentes (incluindo a autoridade nacional de ciber segurança ou o CSIRT nacional se o incidente tiver sido provocado por um ataque informático) para que o incidente e respetivas causas sejam integrados numa base de dados central;
3. Integrar nas medidas preventivas as medidas de proteção e deteção resultantes da análise do operador ou das recomendações transmitidas pelas autoridades nacionais competentes.