CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

outubro 2019

# Roteiro para Capacidades Mínimas de Cibersegurança

O Centro Nacional de Cibersegurança (CNCS) definiu um modelo de capacitação em cibersegurança, visando a melhoria de processos, pessoas e tecnologias nas organizações nacionais, com enfoque especial em PME (Pequenas e Médias Empresas). O presente Roteiro apresenta um conjunto de ações, divididas em 5 fases pensadas para uma adaptação gradual, a implementar em cada organização, seja por meios próprios internos, ou recorrendo a subcontratação ou externalização de soluções. Considera-se que este conjunto de atividades, enquadradas no âmbito do Quadro Nacional de Referência para a Cibersegurança, constitui o plasmar de uma capacidade mínima em cibersegurança, dotando as organizações visadas dos instrumentos mais essenciais que lhe permitirão fazer face às ameaças e perigos do Mundo Digital.

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia

| Classificação | Data | Versão do documento |
|---|---|---|
| TLP WHITE | 29/10/2019 | 1.0 |

| Título |
|---|
| Roteiro para Capacidades Mínimas de Cibersegurança |

| Origem |
|---|
| CNCS – Centro Nacional de Cibersegurança |

| Histórico de Versões | | | |
|---|---|---|---|
| **Versão** | **Data** | **Revisor** | **Comentários/Notas** |
| 1.0 | 29/10/2019 | CNCS | Versão inicial |

# Índice

# GLOSSÁRIO

**CERT**– Computer Emergency Response Team

**CNCS** – Centro Nacional de Cibersegurança

**CSIRT** – Computer Security Incident Response Team

**DNS** – Domain Name System

**FIRST** – Forum of Incident Response and Security Teams

**GNS** – Gabinete Nacional de Segurança

**HIDS** – Host-based Intrusion Detection System

**IDS** – Intrusion Detection System

**IP** – Internet Protocol

**IRT** – Incident Response Team

**LIR** – Local Internet Registry

**NIST** – National Institute of Standards and Technology

**PGP** – Pretty Good Privacy

**PME** – Pequenas e Médias Empresas

**PUA** – Política de Utilização Aceitável

**QNRCS** – Quadro Nacional de Referência para a Cibersegurança

**RAM** – Random Access Memory

**RIPE** – Réseaux IP Européens

**RIPE NCC** – Réseaux IP Européens network coordination centre

**SIEM** – Security Information and Event Management

**SOC** – Security Operations Centre

**SINP** – Sistema Interno de Normas e Políticas

**TIC** – Tecnologias da Informação e Comunicação

**TLP** – Traffic Light Protocol

# 1. Sumário Executivo

Independentemente da quantidade e qualidade dos mecanismos de prevenção instalados, os incidentes de cibersegurança têm-se mostrado mais frequentes e complexos. Neste cenário, interessa preparar a governação interna das organizações, no sentido de elevarem o nível da sua cibersegurança, tendo em conta as suas diversas vertentes[1].

Com o objetivo de apoiar o desenvolvimento de valências mínimas em cibersegurança, sobretudo nas Pequenas e Médias Empresas (PME) e, num âmbito mais alargado, na generalidade das organizações no panorama nacional, o Centro Nacional de Cibersegurança (CNCS) definiu um conjunto de capacidades – técnicas, humanas e processuais – que constituem uma base harmonizada e desejável nesta matéria.

Pretende-se assim proporcionar um instrumento que aumente o nível da organização no domínio da governação de segurança de informação, focado nas competências e capacidades, incluindo ao nível de recursos humanos, para identificar ameaças, percebê-las e reagir face aos riscos do ciberespaço e das atividades em Rede.

Foi assim estabelecido o Roteiro para Capacidades Mínimas em Cibersegurança, constituído por 5 (cinco) fases para que as organizações possam integrar o ecossistema nacional de cibersegurança, criando, simultaneamente, condições para uma melhoria sustentada e coerente dessas capacidades.

Este Roteiro deve ser utilizado como um instrumento complementar ao Quadro Nacional de Referência para a Cibersegurança (QNRCS). Este último é um documento orientador, que aborda de forma abrangente os diversos vetores relacionados com a problemática da segurança nas organizações, seguindo as linhas gerais de normativos como as da família ISO/IEC 27000 ou as que se encontram sob a chancela da NIST. Pretende-se que o Roteiro constitua, no quadro da realidade das PME, a concretização prática das diretrizes que faça sentido implementar, tendo em conta quer a limitação de recursos destas organizações, quer aqueles que devem ser os seus requisitos do ponto de vista da proteção dos seus ativos.

Este documento permitirá desenvolver gradualmente o nível de cibersegurança nas várias organizações. O CNCS disponibiliza também, sem custos associados, um conjunto de instrumentos para ajudar ao desenvolvimento de algumas capacidades. A caraterização destes instrumentos, a sua forma e o seu

[1] Conforme Quadro Nacional de Referência para a Cibersegurança, disponível em https://cncs.gov.pt/recursos/documentos/quadro-nacional-de-referencia-para-a-ciberseguranca/

âmbito podem ser consultados no sítio da Internet do CNCS. Os restantes custos envolvidos na execução deste Roteiro são da responsabilidade da organização, como por exemplo a possível aquisição de ferramentas, instrumentos ou contratação de recursos humanos.

### 1.1. Objetivo

**Este documento apresenta a visão e um conjunto de capacidades preconizadas pelo CNCS como fundamentais ao nível do panorama organizacional nacional, com especial enfoque nas Pequenas e Médias Empresas e em outras organizações que pretendam atingir capacidades mínimas de cibersegurança.**

### 1.2. Roteiro de criação de capacidades mínimas

O processo de desenvolvimento de capacidades mínimas para a cibersegurança permite um desenvolvimento progressivo de cada uma das organizações relativamente ao seu grau de capacitação, percorrendo um conjunto de fases numeradas de 1 (um) a 5 (cinco).

A **primeira fase** é preparatória e o seu objetivo é estabelecer os alicerces para a cooperação entre a organização e o CNCS. Nesta fase, a organização trabalhará para definir um ponto de contacto a articular com o CNCS. Será igualmente identificado o quadro de ameaças que impende sobre a organização, calculando o valor relativo dos seus ativos (bem como o grau de risco a que estão sujeitos), definindo as áreas de segurança distintas, conforme o valor dos respetivos ativos e definindo ainda as respetivas regras de acesso. Deverá ainda identificar as dependências funcionais entre sistemas internos e entre estes e sistemas geridos por terceiros, levando sempre em linha de conta a importância do conjunto para o negócio.

A **segunda fase** irá desenvolver a arquitetura de segurança, focando-se em delimitar as várias áreas de segurança e aplicar regras de controlo de acessos que permitam, por exemplo, detetar tentativas de intrusão em cada uma das zonas de segurança. Ainda nesta fase, a organização deverá agregar num repositório central e correlacionar os eventos de segurança detetados nos diversos elementos de segurança ativa e passiva, bem como agregar, nesse mesmo repositório central, a informação de metadados de comunicações eletrónicas e registos de sistema e aplicações. Em casos específicos, os eventos de segurança relevantes poderão ser comunicados em tempo real ao CNCS para enriquecimento do Quadro Situacional Nacional de Cibersegurança[2].

[2] Disponível em https://www.cncs.gov.pt/projetos/panorama/

A **terceira fase** versará a segurança de dispositivos e aplicações, desenvolvendo na organização mecanismos de deteção e prevenção de ameaças nos dispositivos que tratam os ativos informacionais mais valiosos, incluindo a capacidade de detetar movimentos laterais dos atacantes dentro da mesma zona de segurança. Ainda nesta fase, serão definidas capacidades para a criação de mecanismos de auditoria e alerta de acessos indevidos a bases de dados e outros ativos de elevado valor, mecanismos de alerta para falhas de desempenho e disponibilidade de serviços e mecanismos de controlo e auditoria de acessos sítios de Internet.

A **penúltima fase** consiste em criar procedimentos e políticas que definam e otimizem as capacidades da equipa que estará encarregue da cibersegurança interna, formalizar os procedimentos para operações de cibersegurança, definir as responsabilidades pelas operações de cibersegurança e elaborar um plano de formação individual para os colaboradores envolvidos, desta forma construindo uma estrutura de cibersegurança para toda a organização.

Finalmente, a **quinta fase** destina-se apenas a organizações cuja dimensão, criticidade ou complexidade o justifique e consiste em formalizar equipa(s) dedicada(s) à deteção e resposta de incidentes, com as seguintes capacidades: monitorização e alerta de incidentes de cibersegurança – *Security Operations Centre* (SOC) e/ou *Computer Security Incident Response Team* (CSIRT). A organização deverá ainda colaborar em projetos de desenvolvimento e partilha de informação de cibersegurança de uma forma regular dentro do sector de atividade e, se necessário, com a comunidade de cibersegurança, podendo também participar em exercícios nacionais e internacionais de cibersegurança.

### 1.3. Revisão

O Roteiro para Capacidades Mínimas de Cibersegurança está sujeito a revisões sempre que sejam identificadas oportunidades de melhoria nas capacidades tecnológicas, humanas e processuais associadas aos eixos de intervenção identificados, ou outras alterações que justifiquem a revisão do documento.

### 1.4. Classificação da Informação

Toda a informação partilhada deve seguir os princípios de segurança da informação constantes do modelo TLP (*Traffic Light Protocol*), como publicado no *FIRST Standards Definitions and Usage Guidance,* no que respeita à proteção e disseminação da informação.

## 2. Capacidades mínimas de cibersegurança

### 2.1. FASE 1

A fase preparatória consiste no conjunto de ações que são a base da cooperação entre o CNCS e a organização. Nos objetivos desta fase inicial de preparação incluem-se também a definição dos canais de comunicação entre a organização e o CNCS, a identificação do âmbito material de colaboração/articulação e o arranque dessa mesma colaboração.

No fim desta fase, a organização deverá ter alcançado as seguintes capacidades:

1) Cooperar com o CNCS numa base sistemática, tendo formalizado um protocolo de cooperação, estabelecido canais de comunicação, procedimentos de notificação, e formalizada a nomeação do elemento interno de ligação fundamental para essa cooperação – o RESPONSÁVEL DE SEGURANÇA;

2) Identificar processos de negócio na organização, por forma a identificar prioridades nos respetivos processos e a criticidade inerente aos seus serviços;

3) Dispor de bases normativas internas para a proteção destes ativos críticos e da segurança de informação interna como um todo, através da constituição de uma política de segurança de informação, da determinação de uma cadeia de responsabilidade interna por sistemas e ativos de informação, e da adoção de uma metodologia de gestão de risco que ponha em prática a estratégia da organização para a mitigação de ameaças.

#### 2.1.1. **Ações**

As ações previstas para atingir os objetivos propostos para esta fase são:

| AÇÃO |
|---|
| **A 1.1** - Formalização de Protocolo de Colaboração e Adenda |
| **A 1.2** - Identificação de RESPONSÁVEL DE SEGURANÇA |
| **A 1.3** – Identificação de funções ou atividades críticas |
| **A 1.4** - Estabelecimento de canais de comunicação |
| **A 1.5** - Registo de endereços de IP no LIR (Local Internet Registry) |
| **A 1.6** - Estabelecimento de metodologia de Análise de Risco |
| **A 1.7** – Cadeia de responsabilidade: preparação |
| **A 1.8** – Definição de política de segurança de informação |
| **A 1.9** – Procedimentos de notificação de incidentes |

**A 1.1 - Formalização do Protocolo de Colaboração e Adendas**

O sucesso do processo que é aqui proposto, envolvendo investimentos e disponibilidade de recursos humanos das várias áreas de atividade dentro da organização, depende em grande medida do compromisso e do suporte da respetiva administração ou direção. A evidência desse compromisso é concretizada mediante a formalização de um Protocolo de Colaboração entre a organização e o CNCS e, dependendo dos serviços em que haja cooperação, das respetivas Adendas.

O Protocolo representa a colaboração entre a organização e o CNCS e marca o início do processo de desenvolvimento das capacidades mínimas aqui proposto. No protocolo ficam definidos o RESPONSÁVEL DE SEGURANÇA.

O Elemento de Contacto de Gestão é o ponto de contacto da organização do ponto de vista do negócio e deverá ser capaz de decidir/conduzir todos os assuntos que surjam no âmbito da implementação do Roteiro.

**A 1.2 - Identificação do RESPONSÁVEL DE SEGURANÇA**

O RESPONSÁVEL DE SEGURANÇA é o ponto de contato da organização do ponto de vista técnico/operacional e deverá ser capaz de responder às solicitações da equipa operacional do CNCS (CERT.PT), sendo esperada disponibilidade para contactos de emergência fora do horário de expediente. Este deverá conhecer bem a organização quer do ponto de vista técnico, quer de negócio, devendo ser capaz de reencaminhar internamente as solicitações do CNCS. Por outro lado, é esperada disponibilidade para contactos de emergência fora do horário de expediente. Adicionalmente, a organização poderá indicar um conjunto de técnicos que asseguram, ou poderão vir a assegurar, a função de analistas de cibersegurança. A designação do RESPONSÁVEL DE SEGURANÇA é feita com o preenchimento do Formulário de Identificação de Entidade.

**A 1.3 - Identificação de funções ou atividades críticas**

**QNRCS**
3.5.4
4.3.1

É importante, para a atividade da organização e assim do CNCS e, uma descrição dos serviços críticos prestados pela organização, bem como os endereços IP públicos associados a cada um deles. Esta informação permitirá ao CNCS, a partir de eventos de cibersegurança recolhidos de outras fontes, identificar rapidamente possíveis ameaças ou ataques em curso que envolvam a organização e/ou a função ou atividade associada.

A identificação das funções ou atividades críticas requer a conjugação de uma visão alargada do negócio com uma visão alargada dos processos que o sustentam. Esta ação consiste em definir os mais importantes para a organização, ordená-los por criticidade, identificar potenciais ameaças e consequentes impactos, identificar dependências internas e externas entre sistemas e, finalmente, construir o quadro global de ameaças da organização.

**A 1.4 - Estabelecimento de canais de comunicação**

Alguma da informação trocada por correio eletrónico é sensível, nomeadamente detalhes sobre ameaças, incidentes ou vulnerabilidades que dizem respeito exclusivamente à organização. Para a devida proteção dessa informação é necessário o uso de cifra. Na comunidade de cibersegurança o padrão utilizado é o PGP, pelo que deverá ser criada uma chave PGP associada ao endereço de correio eletrónico da lista de distribuição referida em A 1.1. Opcionalmente, o RESPONSÁVEL DE SEGURANÇA, o Elemento de Contacto de Gestão e cada um dos colaboradores que possam estar incluídos nesse canal de comunicação poderão possuir chaves PGP próprias.

**A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)**

A base de dados do RIPE[3] é a principal fonte de informação de contacto para a comunidade internacional de resposta a incidentes e para o CNCS em particular, a associação de endereços IP a entidades. Por este motivo é extremamente importante que a organização tenha esta informação atualizada junto do *Local Internet Registry* (LIR), que são os membros do RIPE NCC (assim chamados por serem responsáveis pela distribuição de espaço de endereçamento e registo de espaço de endereçamento a nível local). A publicação desta informação no LIR permitirá à organização receber notificações e outra informação de cibersegurança relevante para as redes e sistemas sob sua responsabilidade. Caso não seja possível o registo na base de dados do RIPE, o CNCS opera uma base de dados privativa que poderá ser utilizada pela organização para este efeito.

Assim sendo, a organização deverá atualizar a informação de contacto junto de uma destas duas bases de dados ou pedir ao respetivo fornecedor de Internet para o fazer. O CNCS poderá constar como contacto para resposta a incidentes (objeto IRT) das redes da instituição, apenas durante o tempo necessário para que esta edifique capacidades próprias.

[3] Disponível em https://www.ripe.net/

**A 1.6 - Estabelecimento de metodologia de Análise de Risco**

QNRCS 3.5 4.3.4

A gestão do risco é o processo contínuo de identificação, avaliação e resposta ao risco. Para gerir o risco a organização deve, ainda que aqui explanado de forma sumária, identificar a probabilidade de um evento ocorrer e o impacto que esse evento traria, caso ocorresse. Para efeitos de facilidade na compreensão deste documento, explana-se, de seguida, ainda que de forma sumária, o processo de criação da matriz de risco (probabilidade versus impacto).

Assim, no seguimento da identificação dos serviços críticos, deve ser realizada uma análise de risco que consiste em: (i) identificar as vulnerabilidades associadas a estes serviços e as ameaças a que se encontram expostos; (ii) calcular a probabilidade de concretização da ameaça e o impacto daí esperado; (iii) avaliar a criticidade de cada um dos ativos baseada no impacto decorrente de uma eventual falha de segurança (nível de risco). A gestão de risco consiste na tomada de decisão quanto ao processo de tratamento de cada um dos riscos identificados. Esta decisão pode passar por mitigar, transferir, evitar ou aceitar o risco. Deve aceitar-se o risco apenas quando este não acarreta consequências significativas para a concretização das atividades críticas do negócio. A decisão quanto ao nível de risco aceitável deverá ser tomada ao nível da administração da organização.

A análise do risco irá também ajudar a organização a priorizar as atividades de cibersegurança, fundamentando potenciais investimentos com o foco em atividades especificas que se refletem em resultados concretos de redução do risco.

**A 1.7 - Cadeia de responsabilidade: preparação**

A definição da cadeia de responsabilidade tem início logo na primeira fase e será ajustada ao longo da implementação do Roteiro, ficando formalizada no final da fase 4 (a definição da cadeia de responsabilidade pressupõe também a definição dos privilégios de acesso individual, os quais são definidos em razão das funções desempenhadas e das responsabilidades associadas a cada função).

Esta ação começa com a nomeação de um órgão/equipa/pessoa responsável pela deteção de incidentes de cibersegurança dentro da organização. Esta responsabilidade, que pode ou não ser atribuída ao RESPONSÁVEL DE SEGURANÇA (Elemento de Contato Operacional com o CNCS), deve ser conhecida por toda a organização e ser o ponto de contacto para todos os assuntos

relacionados com a deteção de incidentes de cibersegurança. Cabe ao órgão/equipa/pessoa responsável pela deteção de incidentes de cibersegurança definir e diligenciar pela aprovação dos processos de deteção de incidentes.

**A 1.8 - Definição de política de segurança**

QNRCS 3.6.2

A criação de uma política de segurança de informação da organização é um elemento estruturante para a governação da cibersegurança. Enquanto elemento estratégico, é importante que tenha a aprovação e aceitação da gestão de topo e o envolvimento e compromisso de todos os colaboradores. A sua efetivação verificar-se-á mediante a respetiva tradução em processos e procedimentos específicos a serem posteriormente implementados por cada departamento.

A política de segurança, conjuntamente com a metodologia de análise de risco (ver A1.6), são pilares essenciais de uma abordagem concertada e organizada pela cibersegurança em particular. É importante que aqui se definam as prioridades da organização, bem como os respetivos perfis de risco. As decisões devem ser tomadas, tanto quanto possível, partindo da análise da situação face a esse perfil, constituindo a política de segurança o principal garante das boas práticas e fator de redução de risco e exposição a ameaças nas atividades do dia-a-dia.

**A 1.9 - Procedimentos de notificação de incidentes**

QNRCS 3.6.2

Consiste em criar e fazer aprovar pela direção da organização, um procedimento de notificação de incidente de cibersegurança com impacto nas funções ou atividades identificadas como críticas. O responsável de segurança deverá selecionar a tipologia dos incidentes a incluir no processo de notificação, tendo como referência o catálogo de tipos de incidentes presente na taxonomia de classificação de incidentes. O CNCS presta o apoio necessário na definição e operacionalização deste procedimento de notificação de incidentes de cibersegurança.

## 2.2. FASE 2

A segunda fase consiste no conjunto de ações necessárias para concretizar medidas que são preconizadas em políticas e protocolos estabelecidas na fase anterior, bem como em ações que visem dotar a organização com os principais recursos processuais e técnicos de base para uma defesa eficaz dos seus ativos, quer a nível do perímetro de rede, quer de servidores, postos de trabalho e outros dispositivos. Nesta fase são ainda estabelecidos sistemas processuais internos que garantam a conformidade essencial da organização com requisitos legais e normativos da área de atividade.

Finda esta etapa, a organização deverá, então, ter alcançado as seguintes capacidades:

1) Intensificar o nível de cooperação com o CNCS através da consolidação de canais de comunicação a nível operacional estabelecidos na Fase 1;

2) Ter as bases do desenho de uma arquitetura de rede apropriadamente segmentada, que inclui o recurso a dispositivos de deteção e de defesa de perímetro para filtragem de ameaças provenientes do exterior;

3) Dispor de informação de registo e fluxos de tráfego que permitam uma deteção atempada de ameaças, bem como o diagnóstico a *posteriori* do comportamento dos sistemas internos perante um evento de segurança;

4) Fazer uma apropriada gestão e inventariação de ativos de informação internos, complementada com esquemas ou mapas da rede, dotando a organização da possibilidade de eficientemente lidar com ameaças, contextualizando-as apropriadamente no panorama interno;

5) Prevenir de forma sistemática os riscos de inconformidade com os requisitos legais e normativos ou certificações aplicáveis, estabelecendo um sistema que integra estas prioridades no quadro de conformidade interno, para monitorização e auditoria regular do estado de conformidade;

6) Dispor de resiliência ao nível da disponibilidade e integridade de informação, através da criação e manutenção de procedimentos de *backup* e *restore*, apropriadamente testados,

abrangendo os repositórios de dados da organização que tenham sido para tal identificados em sede de análise de risco;

7) Acautelar a formação dos recursos humanos internos de acordo com um mapa de competências, para que a cibersegurança não seja apenas acautelada por equipas especializadas, mas que seja praticada diariamente no desempenho das funções de cada colaborador, no quadro da política de utilização aceitável de recursos TIC criado nesta fase, bem como do sistema de políticas e normas internas a criar em fase posterior.

### 2.2.1. **Ações**

As **ações** previstas para atingir os objetivos propostos para esta fase são:

| AÇÃO |
|---|
| **A 2.1** – Desenho e implementação da arquitetura e segurança perimétrica |
| **A 2.2** – Implementação de sistema de recolha e armazenamento do fluxo de tráfego |
| **A 2.3** – Comunicação com o CNCS |
| **A 2.4** – Inventariação de ativos / produção de um mapa de rede |
| **A 2.5** – Recolha centralizada de registos (logs) |
| **A 2.6** – Criação de instrumentos de correção ou mitigação de incidentes |
| **A 2.7** – Estabelecimento de conformidade com a legislação aplicável |
| **A 2.8** – Estabelecimento de conformidade com normas aplicáveis à área de atividade |
| **A 2.9** – Criação de política de uso aceitável |
| **A 2.10** – Manutenção de infraestruturas de cópias de segurança e reposição (*Backup/Restore*) |
| **A 2.11** – Mapa de competências e planos de formação |
| **A 2.12** – Treino e sensibilização interna: geral |
| **A 2.13** – Treino e sensibilização interna: gestão |

**A 2.1 - Desenho e implementação da arquitetura e segurança perimétrica**

Aplicando os princípios de uma abordagem por camadas de segurança com base na análise de risco realizada, pretende-se nesta fase desenhar uma nova arquitetura de cibersegurança para a organização, organizar as várias áreas de segurança e identificar as necessidades de deteção de eventos anómalos com origem no exterior e entre zonas de segurança distintas.

Neste sentido deverão existir *firewalls* para controlo dos acessos para/da Internet e entre diferentes zonas de segurança, com regras que minimizem a interação entre camadas. Deverá igualmente existir um Sistema de Deteção e Proteção de Intrusão (IDS/IPS) com visibilidade para

cada zona de segurança, por forma a analisar e monitorizar os padrões de normalidade definidos e/ou definir as regras de monitorização.

O perímetro de rede deve constituir uma primeira linha de defesa contra ameaças externas. A sua configuração e posicionamento devem ser adequados à arquitetura e segmentação da rede. Existem gamas de equipamentos de vários níveis, de acordo com as capacidades e volumes de tráfego a ter em conta, permitindo que cada organização adeque o investimento às suas dimensões e complexidade.

Uma *firewall* configurada adequadamente constitui um dos primordiais elementos de aplicação das políticas internas (ver A 1.8 e A 2.9), fazendo a filtragem do tráfego de acordo com as necessidades da organização e evitando a exposição a protocolos de comunicação e fluxos desnecessários ou perigosos.

O complemento com um sistema de IDS/IPS permite que esta filtragem seja também feita numa base heurística, analisando o conteúdo do tráfego e detetando/bloqueando padrões de ataque conhecidos.

Dada a sua criticidade para o bom funcionamento da arquitetura de sistemas, sugere-se, sempre que possível, a opção pela diversidade em termos de fabricantes/fornecedores de soluções de segurança perimétrica.

**A 2.2 - Implementação de sistema de recolha e armazenamento do fluxo de tráfego**

A tecnologia de exportação e armazenamento do fluxo de tráfego permite recolher, por exemplo através de amostragem, metadados das comunicações que atravessam um equipamento de comunicações eletrónicas. É um instrumento essencial para identificar padrões de comunicação com sistemas potencialmente comprometidos e analisar tráfego considerado malicioso.

O CNCS sugere o armazenamento, com uma amostragem de 1:10, dos metadados de comunicações durante um período mínimo de 1 (um) ano. A recolha dos metadados deve ser efetuada no *router/switch* ou outro equipamento de acesso à Internet. No entanto, se a organização pretender uma maior visibilidade das suas comunicações internas, poderá recolher metadados de outros equipamentos. A implementação de recolha do fluxo de tráfego requer recursos tecnológicos dedicados, cujas características dependem, entre outros fatores, da velocidade de acesso à Internet.

**A 2.3 - Comunicação com o CNCS**

Esta ação pressupõe unicamente a definição do procedimento de comunicação operacional entre a organização e o CNCS. O caderno de procedimentos que resulta desta ação deve ser analisado pelo departamento jurídico e aprovado pela administração da organização.

**A 2.4 - Inventariação de ativos / produção de um mapa de rede**

**QNRCS**
4.3.1

Grande parte das organizações que já executa a função de inventariação de ativos e possui uma *Configuration Management Database* (CMDB) com os mesmos. Muitas outras detêm um catálogo de serviços informáticos aprovados. Esta base de dados fornece parte da informação necessária para o analista de cibersegurança – uma das pessoas responsáveis por conhecer e analisar um incidente – perceber o impacto, direto ou indireto, destes ativos na atividade da organização.

Interessa particularmente registar na CMDB a lista dos principais ativos informáticos de suporte às funções críticas, anteriormente identificadas. Para cada um destes ativos deverá, no mínimo, ser armazenada a informação do endereçamento IP, versões de sistema operativo, versões de aplicações que comunicam com o exterior e dependências funcionais com outros serviços vitais.

Da mesma forma que é necessária uma inventariação de ativos, também é importante manter atualizado um diagrama com as principais infraestruturas de comunicações de dados e os sistemas de suporte aos serviços críticos da organização. Possuir um diagrama de rede é essencial, quer para perceber como se desenvolveram os diversos momentos do ataque, quer para desenhar as soluções de mitigação e identificar a melhor forma de as aplicar. No diagrama de rede deverão constar, no mínimo, todos os segmentos de rede da organização, endereçamento IP usado em cada um deles, endereços IP de interligação, equipamentos de interligação entre os vários segmentos e a indicação das políticas de acesso entres estes. Este diagrama deverá incluir igualmente funções informáticas que sejam externalizadas.

Adicionalmente, a organização deverá ter procedimentos em vigor, com os respetivos controlos para atualização regular dos ativos e do diagrama de rede, com uma periodicidade mínima de 6 meses, ou sempre que ocorram alterações relevantes.

**A 2.5 - Recolha centralizada de registos (*logs*)**

Os *logs* produzidos pelo sistema operativo e pelas aplicações de suporte à atividade são o principal instrumento de análise e investigação de um incidente de cibersegurança. Neste contexto é

essencial que a organização possua um repositório central para estes *logs* com um período mínimo de armazenamento de 1 (um) ano. Em complemento, é importante que cada servidor tenha a capacidade de armazenar os seus próprios *logs* por um período de um mês.

A recolha centralizada de *logs* pressupõe a identificação dos principais sistemas informáticos de suporte aos serviços críticos da organização, a configuração destes sistemas para exportar os registos e a instalação de um servidor dedicado para o seu armazenamento. É igualmente importante incluir a informação de *logging* nos planos de *Backup/Restore* (ver A2.10).

**A 2.6 - Criação de instrumentos de correção ou mitigação de incidentes**

Uma vez identificada a origem de um incidente é necessária a aplicação de medidas corretivas ou de mitigação do mesmo. Para o tipo de situações mais comum pode ser necessário aplicar uma medida de mitigação para colmatar uma falha de segurança num sistema operativo ou aplicação. Pode também ser necessário bloquear determinado tráfego de entrada ou de saída da organização, corrigir uma vulnerabilidade no sítio da internet da organização, ou ainda assegurar que outros sistemas ou dispositivos não foram afetados pela mesma situação ou falha.

Neste contexto, a fase técnica destes instrumentos de correção ou mitigação de incidentes termina quando a organização possui, de forma autónoma ou mediante contratação de serviços, o seguinte:

- Serviços de anti-DDoS (por exemplo contratados ao operador de comunicações eletrónicas);
- Mecanismos de bloqueio de tráfego para IPs e portas específicas (por exemplo, mediante configuração de firewall);
- Mecanismos para identificação de Identificadores de Compromisso (IOC) no parque de dispositivos da organização (por exemplo através de sistema de instalação e execução remota de aplicações);
- Quando aplicável, contratos de manutenção corretiva para todos os componentes de hardware e software presentes na CMDB;
- Quando aplicável, contratos de manutenção corretiva para as aplicações chave na mão de suporte aos serviços críticos.

**A 2.7 - Estabelecimento de conformidade com a Legislação aplicável**

**QNRCS 4.3.3**

A organização deve ter sempre presente e os quadros legais e regulatórios a que está sujeita. A título exemplificativo, empresas de prestação de serviços digitais e outro tipo de organizações com papéis relevantes na sociedade e na manutenção das infraestruturas que prestam serviços essenciais ao país estão no âmbito da Diretiva SRI – Segurança das Redes e dos Sistemas de Informação e assim da Lei 46/2018 de 13 de agosto. Nesse quadro, têm obrigações específicas na governação da sua cibersegurança e na forma como se coordenam e interagem com o CNCS para efeitos da notificação e de resposta a incidentes.

A nível mais abrangente, o Regulamento Geral de Proteção de Dados, em vigor desde maio de 2018, estabelece obrigações comuns a todas as organizações que fazem tratamento de dados pessoais. A respetiva segurança é, segundo o RGPD, dependente da organização interna da cibersegurança, de boas bases de gestão de risco e da assimilação do princípio da Segurança e Privacidade desde a conceção e por defeito.

É importante que a estratégia interna para a conformidade com a legislação aplicável à atividade seja parte da política de segurança (ver A 1.8) e que a metodologia de análise de risco definida (ver A 1.6) tenha em conta esta prioridade, face aos prejuízos decorrentes de uma qualquer não-conformidade.

**A 2.8 - Estabelecimento de conformidade com normas aplicáveis à área de atividade**

**QNRCS 4.3.3**

À semelhança do ponto anterior, a conformidade com normas ou certificações exigidas por Lei ou por força de exigências contratuais ou regulatórias impostas às atividades da organização deve ser um fator prioritário. O incumprimento destas normas pode significar perdas de reputação ou de negócio indesejáveis e potencialmente incomportáveis.

Algumas destas normas podem passar pela aplicação de medidas técnicas ou organizativas no domínio da cibersegurança. Mais uma vez, na linha do ponto anterior (ver A 2.7), essa importância deve ficar plasmada e patente nos instrumentos de governação interna, designadamente, no domínio da cibersegurança, na política de segurança (ver A 1.8) e na metodologia de análise de risco (ver A 1.6). As restantes capacidades elencadas neste documento constituem também elementos de valor acrescentado para a conformidade com as normas aplicáveis em termos de segurança.

## A 2.9 - Criação de política de uso aceitável

A política de uso aceitável (PUA) dos recursos TIC internos é mais um elemento de regulação interna importante. Neste documento devem estar vertidas as linhas de orientação para a boa utilização destes recursos, para que esta seja feita de forma segura por todos os colaboradores com acesso aos mesmos.

É importante ter em conta que grande parte das ameaças a que se expõem as organizações no dia-a-dia estão diretamente relacionados com má utilização dos recursos tecnológicos por parte dos colaboradores. Daí que o estabelecimento adequado de uma PUA para os TIC da organização deva abranger temas como:

- Papéis e Responsabilidades
- Manutenção dos postos de trabalho e ambiente de trabalho
- Correta utilização do e-mail para uso profissional
- Comportamento adequado na navegação na Internet
- Utilização de dispositivos móveis para uso profissional
- Instalação e utilização de *software* aplicacional
- Respeito pelos princípios de ética e pela privacidade e proteção de dados pessoais
- Administração do parque informático e do acesso aos recursos em rede

Para que a aplicação da PUA seja o mais eficaz possível, poderá ser estabelecido um programa de formação interno, que dote os colaboradores da organização com as competências e conhecimentos adequados ao bom desempenho das suas funções (ver A 2.11).

## A 2.10 - Manutenção de infraestrutura de cópias de segurança e reposição (*Backup/Restore*)

Mesmo estabelecendo as bases para a prevenção de incidentes de segurança que afetem a disponibilidade ou integridade da informação em suporte TIC, tais incidentes ocorrerão, provavelmente, uma ou outra vez na vida das organizações. É possível que tais eventos levem à eliminação ou corrupção de dados em sistemas que são importantes para o bom funcionamento da organização. Assim sendo, a existência de mecanismos proporcionais ao risco (ver A 1.6) de tais eventos acontecerem e ao impacto das eventuais perdas deve ser também uma prioridade da organização.

É importante contar com equipamento que permita a salvaguarda de informação considerada prioritária para a organização, possibilitando a respetiva reposição em caso de necessidade. Dependendo da complexidade da infraestrutura da organização, bem como do volume e criticidade dos dados, o *hardware* deve ser dimensionado para dar resposta adequada. Os períodos e abrangência dos *backups* a efetuar devem levar em linha de conta o que for determinado em sede análise de risco (ver A 1.6), assim como os procedimentos adequados à reposição.

Poderá ser adequado, em casos específicos que o justifiquem devido à importância da informação, prever o armazenamento de backups *off-site* (fora das instalações da organização), com recurso a cofres ou infraestruturas resistentes a catástrofes.

No sentido de verificar periodicamente a integridade dos suportes de backup e da qualidade dos mecanismos de reposição, estes devem ser sujeitos a testes periódicos, como parte de um plano no quadro da política de segurança interna (ver A 1.8).

**A 2.11 - Mapa de competências e planos de formação**

A descrição de funções é o pilar fundamental para um sistema de gestão e é a base para processos como o recrutamento, a avaliação de desempenho e o planeamento da formação. Será importante nesta ação identificar, para cada colaborador, a sua atual função e o âmbito das suas responsabilidades, o perfil considerado necessário para esta função, e um plano de formação para conseguir atingir os objetivos para essa função específica.

**A 2.12 - Treino e sensibilização interna: geral**

Depois de criados e aprovados os processos e procedimentos, deverão ser realizadas ações internas de sensibilização em matérias de conduta de cibersegurança e dar a conhecer o caderno de procedimentos. Todos os colaboradores devem receber formação nesta etapa. Podem ser utilizados recursos internos, eventualmente complementados com recursos externos, como sendo o Programa de Sensibilização e Treino do CNCS.

**A 2.13 - Treino e sensibilização interna: gestão**

Além da formação geral (ver ponto anterior), os elementos da gestão e outras pessoas-chave dentro da organização devem ter formação orientada aos principais mecanismos de governação

interna, designadamente no que toca à política de segurança (ver A 1.8) e à metodologia de gestão de risco e sua aplicação prática (ver A 1.6). O principal objetivo destas ações de sensibilização deve ser a mobilização das hierarquias superiores da organização no sentido de perceberem a importância destes instrumentos, e de fazerem com que, no dia-a-dia, os colaboradores e a organização como um todo adotem o que neles está definido.

Também aqui podem ser utilizados recursos internos, eventualmente complementados com recursos externos, como sendo o Programa de Sensibilização e Treino do CNCS.

## 2.3. FASE 3

Esta fase prevê a implementação dos desenhos de arquitetura de rede e defesas perimétricas elaborados na fase anterior, através da instalação de firewall, sistemas de deteção de intrusão em dispositivos e aplicações, nomeadamente *Host-based Intrusion Detection Systems* (HIDS), *honeypots* e controlo de acessos *web* (*proxy*). Esta fase também contempla auditorias de segurança e mecanismos de supervisão, bem como a consolidação de informação de registo e monitorização num sistema integrado de gestão de eventos (SIEM).

Finda esta fase, a organização deverá possui a capacidade de:

1) Proteger o perímetro da sua rede, através da configuração de dispositivos que filtram o tráfego com base em políticas estabelecidas, bem como em reconhecimento e bloqueio de padrões de ataque;
2) Assegurar a integridade e nível de segurança de sistemas aplicacionais internos, através da condução de auditorias e do *hardening* das configurações de equipamentos, aplicações e sistemas operativos de suporte;
3) Gerir centralmente os equipamentos que suportam ativos de informação de forma eficiente, dispondo de sistemas de proteção dos mesmos (HIDS e antivírus) que detetam e bloqueiam intrusões ao nível dos *endpoints*;
4) Garantir o bom funcionamento dos equipamentos de suporte à infraestrutura de rede, através da instalação e manutenção de mecanismos de monitorização, supervisão e alarmística.
5) Controlar e centralizar de forma eficaz a informação de eventos de segurança provenientes dos vários dispositivos e equipamentos de suporte à infraestrutura TIC num sistema SIEM, no sentido de filtrar e organizar esses dados e tornar a informação acionável em termos de segurança;
6) Garantir as capacidades técnicas necessárias, para lidar com ameaças e incidentes de cibersegurança.

### 2.3.1. **Ações**

As **ações** previstas para atingir os objetivos propostos para esta fase são as que de seguida se indicam:

| AÇÃO |
|---|
| **A 3.1** – Definição de procedimentos de operação |
| **A 3.2** – Instalação e configuração de sensores em dispositivos |
| **A 3.3** – Auditoria de segurança e Bases de Dados |
| **A 3.4** – Instalação e configuração de controlo de acessos web – (e.g. serviços proxy) |
| **A 3.5** – Proteção e gestão de equipamentos |
| **A 3.6** – Instalação e configuração de mecanismos de monitorização |
| **A 3.7** – *Hardening* das configurações |
| **A 3.8** – Instalação e configuração de um Security Information and Event Management (SIEM) |
| **A 3.9** – Definição de planos de continuidade de negócio |
| **A 3.10** – Aquisição de competências técnicas |

**A 3.1 - Definição de procedimentos de operação**

Esta ação pressupõe a identificação do procedimento para a deteção de incidentes, procedimentos de atualização de ativos, procedimentos de triagem, procedimentos de análise de observáveis, procedimentos de fluxo de informação interno e de interação com entidades externas. Pressupõe ainda a identificação das responsabilidades e funções para os procedimentos identificados, e que informação, meios e resultados são esperados de cada procedimento, quando cada procedimento deve ser acionado, como se espera que esses mesmos procedimentos ocorram e o porquê (importância e racional) dos mesmos. O caderno de procedimentos que resulta desta ação deve ser validado pelo departamento jurídico e aprovado pela administração da organização.

Devem ser considerados diferentes cenários de atuação, que em si possam produzir alterações de fundo aos próprios fluxos de comunicação e ao papel que pode caber à organização (e também ao CNCS).

**A 3.2 - Instalação e configuração de sensores em dispositivos**

As soluções de *Host-based Intrusion Detection System* (HIDS) acrescentam uma camada de deteção aos tradicionais sistemas de deteção de intrusão colocados na rede.

Esta fase prevê a instalação de sistemas de deteção de intrusão em dispositivos, vulgarmente designados de HIDS, nos sistemas e postos de trabalho que tratam informação mais sensível ou

crítica para a organização. As soluções de HIDS incluem funcionalidades de verificação de integridade, conformidade a políticas, análise comportamental do sistema, deteção de *rootkit* e análise de tráfego de entrada e saída no sistema, entre outros.

Tendo como base a análise de risco realizada, devem ser instalados HIDS em todos os sistemas e postos de trabalho intervenientes nos processos mais sensíveis da organização, nomeadamente nas zonas de segurança onde se encontram, ou de que dependem, os serviços críticos já identificados.

**A 3.3 - Auditoria de segurança a Bases de Dados**

A existência de registos de acesso a base de dados com informação sensível ou crítica configuram uma das melhores medidas dissuasoras de acessos indevidos ou ilícitos. Por outro lado, o armazenamento destes registos durante um período mínimo de 1 (um) ano configura um excelente instrumento para a auditoria e a análise forense em caso de incidente. Esta fase prevê a instalação e configuração de mecanismos de registo e auditoria de acesso a bases de dados com informação sensível ou crítica para a organização.

**A 3.4 - Instalação e configuração de controlo de acessos web – (e.g serviços *proxy*)**

Um serviço proxy vai agir como intermediário entre o utilizador e o seu destino, adicionando estruturas e encapsulamento a sistemas distribuídos. Irá atuar no sentido de uma deteção (e, eventualmente, prevenção) eficaz de acessos a sistemas de comando e controlo (C&C) ou repositórios de dados exfiltrados através da Internet.

**A 3.5 - Proteção e gestão de equipamentos**

Instalação de antivírus com visibilidade sobre todo o parque informático, ou em alternativa, no mínimo para os serviços críticos e para os dispositivos dos administradores de sistemas, uma vez que as máquinas dos administradores de sistemas devem ser tratadas com nível máximo de criticidade por terem acesso a todos os recursos que processam e armazenam a informação da organização.

No sentido de tornar a gestão eficaz, é importante que permita o controlo centralizado e que sejam aplicados automatismos para atualização regular das respetivas assinaturas, bem como agendamento de análises periódicas aos *endpoints* para deteção de infeções.

Os dispositivos de comunicação e armazenamento móveis são muitas vezes esquecidos nas prioridades da cibersegurança. No entanto, trata-se já de equipamentos tidos como

indispensáveis por muitas organizações e são ferramentas de trabalho que devem estar ao abrigo da política de segurança (ver A 1.8) e da política de utilização aceitável de recursos TIC (ver A 2.9) e, consequentemente, do Sistema Interno de Normas e Políticas (ver A 4.3).

Adicionalmente deve ser criada uma política BYOD atenta à manutenção e gestão deste tipo de dispositivos que deverá considerar, no mínimo, os seguintes aspetos:

- Armazenamento de dados da organização em dispositivos móveis corporativos e pessoais.
- Acondicionamento, circulação e eliminação de dispositivos de armazenamento móvel.

Independentemente da política de BOYD, os dispositivos móveis devem estar sujeitos a:

- Inclusão de dispositivos móveis na proteção de *endpoints* (ver A 3.4).
- Aplicação de criptografia ao conteúdo de dispositivos móveis contendo informação corporativa.
- Inclusão de HIDS em dispositivos móveis.

**A 3.6 - Instalação e configuração de mecanismos de monitorização**

Esta fase prevê a instalação e configuração de um sistema de monitorização dos principais ativos de rede e sistemas de suporte às atividades da organização. Tipicamente, um sistema de supervisão abrange a leitura regular de variáveis de sistema diretamente nos equipamentos e sistemas, como o espaço do disco, memória RAM, temperatura de componentes críticos e volume de tráfego, bem como testes à disponibilidade e bom funcionamento, incluindo tempos de resposta aceitáveis do ponto de vista dos utilizadores do serviço.

Este sistema deverá medir indicadores de disponibilidade e de qualidade dos equipamentos e serviços, espoletando alertas sempre que o valor medido ultrapasse os parâmetros normais de funcionamento (que deverão ser definidos pela organização).

**A 3.7 - *Hardening* das configurações**

Este é um processo de robustecimento alinhado com um mapeamento das ameaças, das ações de mitigação dos riscos e com a execução das atividades corretivas, com foco na infraestrutura. Passa, muitas vezes, pela alteração e aplicação de restrições às configurações, quer a nível de sistema operativo, quer aplicacional, no sentido de permitir apenas as funcionalidades e comunicações estritamente necessárias, e torná-las tão seguras quanto possível.

Um processo de *hardening* pode também incluir a aplicação e manutenção regular (previamente validada) de atualizações do *firmware*, dos sistemas operativos e das aplicações, a revisão das permissões de acesso aos sistemas e a revisão da segurança nos acessos, entre outros.

**A 3.8 - Instalação e configuração de um *Security Information and Event Managment* (SIEM)**

Com o intuito de obter uma visão holística da segurança da informação crítica da organização, a mesma deverá possuir um sistema de gestão e correlação de dados e eventos, conhecido como SIEM, que agrega os registos (*logs*) mais relevantes produzidos pelos ativos e pelas aplicações de suporte à atividade, facilitando a análise em tempo real e acelerando a tomada de ações defensivas.

Para não sobrecarregar o SIEM, sugere-se a utilização de um outro repositório que funcione como repositório dos registos, para que seja feita uma filtragem e normalização de dados inicial, antes dos registos serem enviados para o SIEM.

Quer o repositório quer o SIEM deverão guardar os registos por um período mínimo de 1 (um) ano (histórico) e 2 (dois) anos de estatísticas. Em complemento, é importante que cada ativo (por exemplo, um servidor) tenha a capacidade de armazenar os seus próprios registos por um período de um mês. A recolha centralizada de registos pressupõe a identificação dos principais sistemas informáticos de suporte aos serviços críticos da organização, a configuração destes sistemas para exportar os registos e a instalação de um serviço dedicado ao seu armazenamento.

Para organizações cuja dimensão e criticidade do negócio o justifiquem, deverá ser equacionada a possibilidade de esta contribuir para o sistema agregador de informação de perceção situacional disponibilizado pelo CNCS (sistema Panorama). A organização poderá entrar em contacto com o CNCS no sentido de se avaliar a aplicabilidade desta medida.

**A 3.9 - Definição de planos de continuidade de negócio**

O Plano de Continuidade de Negócio é um elemento complementar importante à política de segurança interna (ver A 1.8). Usualmente, este plano é, ele próprio, constituído por outros planos, designadamente os de Contingência, Gestão de Crises, Recuperação de Desastres e Continuidade operacional.

Devem fazer parte deste plano os elementos essenciais que permitam à organização continuar em operação perante um qualquer desastre ou incidente que cause (ou tenha potencial para causar) uma disrupção significativa ou até total na atividade.

O plano deve fazer referência, no mínimo, a:

- Critérios de ativação
- Contactos de pessoas ou organizações-chave
- Papéis e responsabilidades na ativação
- Procedimentos a adotar na ativação
- Cadeia de pessoas ou departamentos a envolver nos fluxos de informação
- Instalações alternativas
- Serviços alternativos
- Recursos a mobilizar (internos e externos)
- Eventuais procedimentos para reposição de sistemas ou serviços essenciais

**A 3.10 - Aquisição de competências técnicas**

A análise de artefactos informáticos é uma das principais tarefas de um analista de cibersegurança no contexto da resposta a incidentes. Assim sendo, é essencial que as pessoas indicadas pela organização para realizarem esta função recebam periodicamente formação específica nesta matéria, de forma a desenvolverem, com autonomia, investigações forenses em sistemas operativos (sendo os mais vulgares Windows, MacOS e Linux).

Do mesmo modo, o analista de cibersegurança pode ter a necessidade de identificar ou confirmar a origem de um ataque, ou, ainda, determinar o momento em que este ocorreu. Para esse efeito poderá ter que recorrer a informação de metadados de comunicações armazenada ou realizar uma captura de tráfego específica. Assim, o analista de cibersegurança deverá receber formação específica na utilização das principais ferramentas de análise de *flows*, captura de tráfego e análise de tráfego capturado.

É igualmente importante dotar os analistas de cibersegurança indicados pela organização com as noções básicas em resposta a incidentes, o seu enquadramento nas principais normas nacionais e internacionais de segurança da informação, as noções básicas de gestão de vulnerabilidades, os meios de comunicação interna e externa dentro das comunidades de cibersegurança e dar a conhecer as ferramentas comummente usadas para a resposta a incidentes.

Finalmente, de forma a realizarem as suas várias funções dentro do quadro jurídico vigente e articularem com eficácia com todas as autoridades relevantes nesta matéria, os analistas de cibersegurança deverão ter as noções básicas em aspetos jurídicos relacionados com a sua

atividade. Entre outros, esta ação de formação incidirá nos aspetos legais relativos à recolha e salvaguarda de prova, comunicação com os órgãos de polícia criminal e partilha de informação de cibersegurança.

### 2.4. FASE 4

A quarta fase representará, para a maior parte das organizações, o culminar do processo de capacitação interna no domínio da cibersegurança. Nesta fase procurar-se-á consolidar e formalizar alguns processos e normativos internos estabelecidos em fases precedentes, bem como complementar a formação de recursos humanos e as proteções a nível tecnológico de equipamentos que contenham ou permitam a circulação em rede de informação corporativa. É também nesta fase que se estabelece a gestão de processos de mudança.

Assim sendo, após a conclusão das ações propostas, a organização deverá ter capacidade para:

1) Gerir eficientemente os processos operacionais de segurança interna através da constituição formal de procedimentos, bem como gerir apropriadamente as responsabilidades por processos e ativos de informação internos, através da formalização da cadeia de responsabilidades;

2) Integrar as políticas e normativos definidos em fases anteriores dentro de um quadro de gestão apropriado, ao abrigo de um sistema que zela pela sua manutenção, melhoria contínua e aplicação;

3) Garantir a manutenção da aplicação da metodologia de gestão de risco previamente definida, instituindo a prática periódica de condução de análise de risco na medida do que for considerado apropriado para a dimensão, complexidade e criticidade da informação a proteger, e contemplando a condução de simulacros para testar devidamente os dispositivos internos de resposta a ameaças;

4) Gerir apropriadamente processos de mudança, incluindo a aplicação de *patches* e atualizações de segurança regulares, no quadro de um sistema que garanta a compatibilidade destas alterações com o bom funcionamento dos sistemas aplicacionais e um nível de elevada proteção dos ativos de informação;

5) Abranger a segurança de dispositivos móveis e outros componentes em rede no quadro das medidas tecnológicas e processuais que garantem um elevado nível de proteção da informação;

6) Condicionar a entrada em produção de sistemas e aplicações mediante a aplicação de testes de segurança e consequente aceitação por parte de uma equipa especializada;

7) Dispor de colaboradores sensibilizados nas áreas gerais de cibersegurança ligadas ao desempenho das respetivas funções profissionais, assegurando a aplicação de boas práticas neste domínio no dia-a-dia das atividades da organização.

8) Dispor de hierarquias sensibilizadas para a importância da manutenção de um elevado nível de preparação e defesa ao nível da cibersegurança, assegurando que zelam pela manutenção e melhoria contínua dos sistemas de suporte a políticas, processos e tecnologias que permitem essa proteção, e que zelam pela adoção de uma cultura de segurança na sua organização.

### 2.4.1. **Ações**

As **ações** previstas para atingir os objetivos propostos para esta fase são as que de seguida se indicam:

| AÇÃO |
|---|
| **A 4.1** – Cadeia de responsabilidades: formalização |
| **A 4.2** – Definição do Sistema Interno de Normas e Políticas (SINP) |
| **A 4.3** – Análise de risco - reavaliação |
| **A 4.4** – Simulacro |
| **A 4.5** – Definição de procedimentos de reação a incidentes |
| **A 4.6** – Treino e sensibilização interna: SINP |
| **A 4.7** – Testes de aceitação se serviços |
| **A 4.8** – Mecanismos de engodo (*honeypots*) |
| **A 4.9** – Gestão de mudanças e atualizações |

**A 4.1 - Cadeia de responsabilidades: formalização**

A definição da cadeia de responsabilidades teve início na primeira fase e ficará formalizada agora, na quarta fase. A definição da cadeia de responsabilidades pressupõe também a definição dos privilégios de acesso individual, devendo ser aprovada ao mais alto nível da organização e ser do conhecimento de todos os colaboradores.

**A 4.2 - Definição do Sistema Interno de Normas e Políticas (SINP)**

Esta ação consiste em regular e normalizar os termos do funcionamento interno da organização, através da criação de um conjunto de políticas de segurança, normas e boas práticas internas - Sistema Interno de Normas e Políticas - a ser adotado transversalmente por todos os colaboradores da organização e que deverá impulsionar e apoiar todos os colaboradores na execução diária da sua atividade.

O SINP pretende igualmente constituir-se como um instrumento dinâmico que procura, numa perspetiva proactiva e de partilha de conhecimento, permitir a todos os colaboradores participar na construção dos termos da atividade da organização através da identificação de áreas e processos que eventualmente careçam de regulação mais apurada ou distinta, ou através da recolha, reconhecimento e divulgação de boas práticas e processos eficientes/eficazes que resultem da experiência e área de conhecimento especial de cada colaborador.

Os colaboradores devem ainda adotar, no tratamento de informação, um comportamento adequado ao objetivo de incremento da produtividade, integridade funcional e tecnológica, e segurança dos recursos e informação.

**A 4.3 - Análise de risco – reavaliação**

Uma vez que a gestão de risco é um processo contínuo, para avaliar novamente a organização no final da implementação do Roteiro será realizada uma reavaliação da análise de risco realizada na fase 1.

Depois do fim da implementação do Roteiro, sugere-se que seja feita recorrentemente esta análise, com uma periodicidade anual (mínima), pela organização.

**A 4.4 - Simulacro**

De forma autónoma ou com o apoio do CNCS, a organização deverá realizar simulacros de incidentes de cibersegurança para avaliação do nível de sensibilização dos seus colaboradores e do grau de preparação dos analistas de cibersegurança para lidar com os tipos de incidente mais comuns.

Estes simulacros deverão ocorrer, pelo menos, anualmente e devem testar as capacidades implementadas neste documento.

**A 4.5 - Definição de procedimentos de reação a incidentes**

Esta ação pressupõe a identificação dos tipos de ataque mais comuns e a criação de um procedimento para a respetiva mitigação ou resolução. O caderno de procedimentos que resulta desta ação deve ser aprovado pelo departamento jurídico e pela administração da organização. Também deve ser criado um procedimento interno para notificação de incidentes que indique como um colaborador deve proceder perante um incidente ou um evento suspeito.

**A 4.6 - Treino e sensibilização interna: SINP**

Sendo o SINP um sistema de que afeta transversalmente todos os setores da organização, é fundamental que todos os colaboradores, principalmente os que ocupem cargos de chefia ou coordenação, recebam formação que lhes dê o enquadramento adequado. Esta formação deverá ser ministrada pelos responsáveis pela manutenção do SINP, e deverá permitir que o público-alvo seja capaz de incorporar nos seus processos de trabalho diário as normas ou diretrizes presentes no sistema.

**A 4.7 - Testes de aceitação de serviços**

Deve ser parte da postura defensiva em matéria de cibersegurança das organizações a adoção de práticas que implementem o princípio de segurança na conceção e por defeito *(security by design and by default*), tal como já anteriormente referido. Como complemento essencial deste princípio, é importante que os serviços disponibilizados pela organização, assentes em recursos TIC, sejam submetidos a testes de segurança antes de passarem a produção e serem disponibilizados ou expostos à utilização generalizada.

Estes testes devem ser conduzidos por equipas especializadas em segurança ofensiva, e não devem ser confundidos com testes funcionais. Os objetivos são o de submeter as aplicações, serviços e sistemas a ataques de vários tipos e intensidades, analisar o respetivo comportamento perante esses ataques, propor ações para remediar eventuais problemas detetados e, em última instância, aprovar o sistema quando estiver em condições aceitáveis.

**A 4.8 - Mecanismos de engodo (*honeypots*)**

As proteções de perímetro elencadas (ver A 2.1) serão um filtro importante para evitar ou bloquear a grande maior parte das ameaças. No entanto, é prudente assumir uma postura de prevenir qualquer eventualidade, e ter em conta a possibilidade de estes mecanismos serem ultrapassados.

Um dos primeiros sinais de atividade maliciosa, após a intrusão inicial, é a tentativa de estabelecer movimentos laterais, que permitam ao atacante estender o seu controlo a outros serviços ou sistemas dentro da rede. Os vulgarmente designados *honeypot* são sistemas dedicados que mimetizam funções informáticas de uma organização e que funcionam como engodo para atrair os atacantes, permitindo desta forma identificar os seus métodos de ataque e avaliar as suas capacidades. Tipicamente um *honeypot* mimetiza serviços comuns como o website ou o servidor de correio eletrónico da organização. É usual utilizarem-se estes sistemas como meio de

investigação do estado-da-arte de tecnologia e procedimentos de ataque em cibersegurança. Estes ambientes podem também ser utilizados como uma defesa, no sentido de detetar uma intrusão ou ataque até então despercebido. Se o *honeypot* mimetizar sistemas sensíveis dentro da respetiva zona de segurança e desligado da Internet, toda a alarmística gerada representa um movimento lateral de um atacante que já se encontra dentro da rede da organização.

Esta fase pressupõe a instalação e configuração de um *honeypot* dentro das zonas de segurança com ativos que processam ou armazenam informação sensível.

**A 4.9 - Gestão de mudança e atualizações**

A apropriada gestão de processos de *patching*, atualizações e, de forma geral, da mudança em sistemas computacionais é crucial para manter o melhor nível de segurança possível. Deve ser sublinhado que grandes incidentes de segurança do passado recente com impacto em larga escala tiveram essa dimensão graças à falta de atualizações de postos de trabalho, servidores ou outros ativos de suporte a infraestruturas de TIC nas organizações.

Se, por um lado, é certo que as aplicações e sistemas operativos devem ser mantidos tão atualizados quanto possível, é necessário não esquecer que estas atualizações podem acarretar consequências indesejáveis, tais como incompatibilidades que põem em causa o bom funcionamento dos sistemas em que se inserem.

Assim, é fundamental que a organização estruture os seus processos no sentido de planear adequadamente os processos de mudança, acautelando os riscos que forem identificados nos mesmos (ver A 1.6) e determinando os recursos necessários para que estes processos sejam adequadamente efetuados, passando por uma cadeia de aprovação interna.

As boas práticas em processos de alteração estão descritas, por exemplo, em *Information Technology Infrastructure Library* (ITIL). Estas boas práticas de processos de alteração devem ser estabelecidas no quadro do Sistema Interno de Normas e Políticas (ver A 4.3).

## 2.5. FASE 5

A quinta fase destina-se a organizações cuja dimensão, criticidade ou complexidade o justifique, e compreende, entre outras, as ações necessárias para a operacionalização de um SOC e/ou CSIRT na organização. A decisão de criação de um SOC ou CSIRT deve ter em conta a dimensão da organização, a importância estratégica dos seus ativos informacionais, a capacidade financeira e o histórico de incidentes. Por este motivo, a execução desta fase pode ser objeto de avaliação conjunta entre a organização e o CNCS.

No final desta fase é suposto que a organização reúna o seguinte conjunto de competência internas:

1) Dispor de um responsável máximo pela segurança de informação (*Chief Information Security Officer* - CISO), que deverá estar no topo da hierarquia que controla a cibersegurança e as equipas de deteção e resposta a incidentes de segurança (SOC e/ou CSIRT), e constituindo o culminar da materialização de uma estrutura hierárquica independente e autónoma dedicada à gestão da segurança de informação dentro do organograma da organização;

2) Assegurar a eficaz gestão de incidentes e vulnerabilidades, através da criação de uma ou mais equipas especializadas (SOC ou CSIRT), após adequada formalização dos seus normativos de constituição interna, plano de atividades e aprovação de orçamento próprio. A posterior integração desta equipa na comunidade de cibersegurança nacional (ou até internacional) tenderá a elevar o nível de cooperação em casos que exijam mitigação de impacto de incidentes ou em matéria de prevenção dos mesmos, sendo que essa integração acelerará, certamente, a tomada de medidas concertadas no quadro de uma rede de confiança entre organizações congéneres;

3) Contar com um sistema de gestão de crise nos processos internos, que reduzirão o tempo de reação e elevarão a eficácia de combate a desastres, incidentes ou eventos de uma magnitude que possa causar um impacto catastrófico na organização.

### 2.5.1. **Ações**

As **ações** previstas para atingir os objetivos propostos para esta fase são as que de seguida se indicam:

| AÇÃO |
|---|
| **A 5.1** – Nomear um CISO |
| **A 5.2** – Estabelecer um serviço de gestão de vulnerabilidades |
| **A 5.3** – Estabelecer e implementar um plano de auditorias |
| **A 5.4** – Definir a missão, a comunidade servida e o portfólio de serviços do CSIRT |
| **A 5.5** – Elaborar e fazer aprovar o plano e o orçamento para o CSIRT |
| **A 5.6** – Montar e anunciar o CSIRT |
| **A 5.7** – Estabelecer um sistema de gestão de Crise |
| **A 5.8** – Afiliação nas comunidades nacionais e internacionais de CSIRT |
| **A 5.9** – Participação num exercício nacional de cibersegurança |

**A 5.1 - Nomear um CISO**

QNRCS 5.2

A nomeação de um CISO destina-se a atribuir a gestão da segurança de informação a um responsável máximo e, assim, assegurar que esta tem uma gestão própria e independente, assim como um âmbito de intervenção transversal. A governação da segurança de informação numa organização com elevado grau de complexidade ou dimensão necessita deste destaque e autonomia como contraponto a outros legítimos interesses relacionados com a gestão interna da organização.

O CISO deve ser o topo da hierarquia no que toca à governação de segurança, e o elemento da direção a quem reporta o SOC ou CSIRT.

**A 5.2 - Estabelecer um serviço de gestão de vulnerabilidades**

O serviço de gestão de vulnerabilidades é uma das capacidades que se considera indispensável no quadro de competências do SOC ou CSIRT (ver A 5.3). Sendo o SOC e CSIRT serviços reativos, embora com atribuições distintas, a componente preventiva não pode ser descurada. Um serviço de gestão de vulnerabilidades engloba, geralmente, duas componentes: deteção e mitigação.

A organização deve estabelecer um serviço que, com a periodicidade adequada, execute pesquisa de vulnerabilidades dentro da sua rede. Deve ser um serviço que recorre essencialmente a ferramentas automatizadas, a complementar, nos casos que mereçam atenção especial, com interação humana de técnicos especializados. Para além desta componente periódica, o serviço de deteção também deve estar disponível, sempre que necessário, como parte do portfólio de serviços para apoio aos testes de aceitação de novos serviços (ver A 4.9).

Logicamente, para que a deteção tenha consequências, há que acautelar a componente de mitigação. Nesta fase do ciclo de vida das vulnerabilidades, o SOC ou CSIRT deverá lidar com os responsáveis por sistemas vulneráveis, no sentido de que a remediação ou eliminação da vulnerabilidade seja efetivada e assim acautelando que os serviços não são negativamente afetados no processo. Trata-se de um processo tipicamente moroso e complicado, pois estão em causa equilíbrios de ecossistemas tecnológicos cujo funcionamento pode ser posto em causa por incompatibilidades resultantes de *patching*, atualizações ou outras operações de mitigação, ou seja, devem contemplar os requisitos referidos na gestão de mudança (ver A 4.11).

**A 5.3 - Estabelecer e implementar um plano de auditorias**

A execução de um plano de auditorias tem o objetivo de pôr à prova os controlos de segurança implementados na organização. O SINP (ver A 4.2), se existir, poderá ser um guião apropriado para as auditorias a efetuar, uma vez que ao seu abrigo deverão estar as políticas de segurança aplicáveis, de onde emanarão os controlos que devem ser alvo de auditoria.

Pretende-se, pois, que as auditorias visem os processos de negócio da organização, de acordo com as prioridades e criticidades previamente definidas (ver A 1.3 e A1.6). É aconselhável que eventuais auditorias internas sejam complementadas com auditorias externas, a cargo de empresas especializadas, e que o plano contemple, no mínimo, uma periodicidade anual para a realização de uma auditoria geral e abrangente, sem prejuízo de outras auditorias de cariz mais específico que podem ser realizadas com períodos mais frequentes, ou até mediante necessidade (*on demand*).

**A 5.4 - Definir a missão, a comunidade servida e o portfólio de serviços do CSIRT**

QNRCS 5.4

A primeira ação para a constituição de um CSIRT na organização passa por definir a visão para esse mesmo CSIRT. Consiste em definir e validar, com as partes interessadas, uma definição clara da missão, uma identificação da comunidade servida e o desenho do portfólio de serviços adequado para atingir os objetivos propostos.

Do portfólio de serviços deverá constar, no mínimo, o tratamento de incidentes de cibersegurança e a gestão de vulnerabilidades.

Para a construção desta visão contribuem muitos dos entregáveis produzidos nas fases anteriores, nomeadamente a gestão de ativos, a definição de uma cadeia de responsabilidade e os processos de mitigação de incidentes.

**A 5.5 - Elaborar e fazer aprovar o plano e o orçamento para o SOC ou CSIRT**

Um SOC ou CSIRT deve ter uma estrutura capaz e sustentável. Para esse efeito é necessária a aprovação, por parte da direção da organização, de um plano de ação e orçamento para montar e operar a equipa.

O sucesso do SOC ou CSIRT depende da objetividade da sua missão e da adequação dos meios e dos instrumentos para atingir os seus objetivos.

Deste plano deverá constar uma proposta de enquadramento funcional dentro da estrutura orgânica da organização, a definição já referida da missão, da comunidade servida e portfólio de serviços, não excluindo o consequente plano de investimentos para a montagem inicial da função SOC ou CSIRT, o plano de formação e capacitação para os recursos humanos alocados e/ou a contratar, o plano de deslocações de representação e participação nas comunidades de cibersegurança e o calendário para a sua operacionalização.

**A 5.6 - Implementar e anunciar o CSIRT**

QNRCS 5.3

Aprovado o plano de ação, dá-se início à operacionalização do CSIRT. Esta ação prevê a aquisição e montagem das infraestruturas técnicas e operacionais, bem como a afetação, requalificação ou contratação dos recursos humanos necessários.

Tipicamente um CSIRT precisa de um sistema de registo de ocorrências e comunicações, de canais de comunicação (telefone, correio eletrónico ou portais web), de mecanismos de cifra (por exemplo, PGP) e de um conjunto de ferramentas de suporte à análise forense de artefactos. A maior parte destas ferramentas são de acesso livre e gratuito.

De forma a automatizar processos, e após uma avaliação conjunta entre a organização e o CNCS, poderá ser possível a integração do sistema de ocorrências da organização com os mecanismos de disseminação de eventos e de alertas do CNCS, utilizando uma ontologia e uma taxonomia comuns.

Por outro lado, é necessário formar os recursos humanos afetos à função CSIRT com as competências técnicas necessárias. Dependendo dos objetivos, as capacidades necessárias são: procedimentos de tratamento de incidentes, análise técnica de tráfego, análise técnica de artefactos e análise técnica de malware.

Por último importa anunciar o CSIRT à comunidade servida. Uma equipa de resposta a incidentes opera sobre as notificações internas e externas que lhe chegam, donde é essencial que o CSIRT se

dê a conhecer aos seus utilizadores, bem com às várias comunidades de cibersegurança nacionais e internacionais. Para esse efeito é essencial assegurar presença regular nos principais fora de cibersegurança e participar ativamente nos seus planos de trabalhos.

O CSIRT deve, igualmente, solicitar ao prestador de serviços de comunicações eletrónicas a publicação de um objeto IRT (*Incident Response Team*) junto do LIR.

**A 5.7 - Estabelecer um sistema de gestão de crise**

A gestão de crise será essencial para lidar com grandes incidentes de segurança, que ponham em causa o negócio ou serviços críticos da organização. O estabelecimento de um sistema integrado, com recurso a um comité interno de crise formado por pessoas-chave dentro da organização, poupará tempo na tomada de decisões e assegurará a salvaguarda de todos os stakeholders internos.

Enquanto equipa de resposta a incidentes, o CSIRT deve ser uma parte importante deste sistema, mas certamente que não será o único, tendo em conta a escala que a gestão de crises tipicamente representa, em termos do âmbito de potencial ou efetivo impacto.

Há que acautelar ainda, em sede dos planos de continuidade de negócio (ver A 3.10), que esteja adequadamente refletido o papel e intervenção do sistema de gestão de crises neste âmbito.

**A 5.8 - Afiliação nas comunidades nacionais e internacionais de CSIRT**

O sucesso de um CSIRT depende da sua boa integração nas várias comunidades de cibersegurança e das relações de confiança que aí são criadas.

Neste contexto, o CSIRT da organização deverá afiliar-se e participar ativamente nos programas de trabalhos das comunidades nacionais de CSIRT, tais como a Rede Nacional de CSIRT e, se adequado, do Task-Force for *CSIRTs in Europe* (TF-CSIRT) ou *Forum of Incident Response and Security Teams* (FIRST). Adicionalmente, recomenda-se a participação em fora nacionais e/ou internacionais sectoriais, tais como o FI-ISAC (*Financial Services – Information Sharing and Analysis Centre*) para o sector bancário.

## A 5.9 - Participação em exercícios de cibersegurança

Os exercícios de cibersegurança servem dois objetivos importantes: testar as capacidades, mas principalmente os procedimentos para resposta a incidentes, e melhorar a articulação interna e externa com as partes interessadas.

O CSIRT da organização deve participar num exercício de cibersegurança pelo menos uma vez por ano, seja o mesmo de âmbito nacional ou internacional.

## 3. Conclusões

O presente Roteiro serve de referência nacional para a criação de capacidades mínimas no domínio da cibersegurança, promovendo o equilíbrio do ecossistema da cibersegurança em Portugal.

Este documento visa igualmente a discussão nacional e internacional das temáticas em causa e, como tal, não pretende ser uma versão estática, mas sim dinâmica, prevendo-se a constante atualização com versões aperfeiçoadas.

Ao longo das cinco fases aqui caracterizadas, as ações que se elencam visam a capacitação da organização com recursos próprios. Deve referir-se, no entanto, que, dependendo da análise de risco e eficiência a nível de custos, resultados equivalentes poderão ser obtidos recorrendo a subcontratação de serviços, equipamentos ou mesmo de recursos humanos.

Relativamente às ações aqui preconizadas, deve acrescentar-se que, mesmo nos pontos onde não é referida esta via explicitamente, a opção pela subcontratação ou externalização de soluções pode e deve ser equacionada pela organização como alternativa válida à implementação com recursos internos. Também no domínio da intervenção humana, o mercado oferece soluções de resposta a incidentes, deteção e monitorização contínua de segurança.

A importância da análise de risco na tomada de decisões sobre a forma de implementação (in house vs. subcontratar) permitirá procurar o equilíbrio entre eventuais desvantagens financeiras e logísticas em dispor de meios próprios com potenciais impactos na segurança como um todo, ou optar-se pela externalização ou subcontratação. Esses potenciais impactos poderão advir da dependência de organizações externas, eventuais riscos de confidencialidade e problemas de portabilidade. É importante, pois, que estas decisões sejam tomadas conscientemente pela organização, tendo presente a criticidade dos ativos de informação que pretende proteger, no enquadramento das suas capacidades financeiras.

# ANEXOS

## Anexo I – Sumário de ações

| | AÇÃO |
|---|---|
| A 1.1 | Formalização de Protocolo de Colaboração e Adenda |
| A 1.2 | Identificação de RESPONSÁVEL DE SEGURANÇA |
| A 1.3 | Identificação de funções ou atividades críticas |
| A 1.4 | Estabelecimento de canais de comunicação |
| A 1.5 | Registo de endereços de IP no LIR (Local Internet Registry) |
| A 1.6 | Estabelecimento de metodologia de Análise de Risco |
| A 1.7 | Cadeia de responsabilidade: preparação |
| A 1.8 | Definição de política de segurança de informação |
| A 1.9 | Procedimentos de notificação de incidentes |
| A 2.1 | Desenho e implementação da arquitetura e segurança perimétrica |
| A 2.2 | Implementação de sistema de recolha e armazenamento do fluxo de tráfego |
| A 2.3 | Comunicação com o CNCS |
| A 2.4 | Inventariação de ativos / produção de um mapa de rede |
| A 2.5 | Recolha centralizada de registos (*logs*) |
| A 2.6 | Criação de instrumentos de correção e mitigação de incidentes |
| A 2.7 | Estabelecimento de conformidade com a legislação aplicável |
| A 2.8 | Estabelecimento de conformidade com normas aplicáveis ao setor |
| A 2.9 | Criação de política de uso aceitável |
| A 2.10 | Manutenção de infraestrutura de cópias de segurança e reposição (*Backup/Restore*) |
| A 2.11 | Mapa de competências e planos de formação |
| A 2.12 | Treino e sensibilização interna: geral |
| A 2.13 | Treino e sensibilização interna: gestão |
| A 3.1 | Definição de procedimentos de operação |
| A 3.2 | Instalação e configuração de sensores em dispositivos |
| A 3.3 | Auditoria de segurança a Bases de Dados |
| A 3.4 | Instalação e configuração de controlo de acessos web – (e.g serviços *proxy*) |
| A 3.5 | Proteção e gestão de equipamentos |
| A 3.6 | Instalação e configuração de mecanismos de monitorização |
| A 3.7 | Hardening das configurações |
| A 3.8 | Instalação e configuração de um *Security Information and Event Managment* (SIEM) |

| | |
|---|---|
| A 3.9 | Definição de planos de continuidade de negócio |
| A 3.10 | Aquisição de competências técnicas |
| A 4.1 | Cadeia de responsabilidades: formalização |
| A 4.2 | Definição do Sistema Interno de Normas e Políticas (SINP) |
| A 4.3 | Análise de risco – reavaliação |
| A 4.4 | Simulacro |
| A 4.5 | Definição de procedimentos de reação a incidentes |
| A 4.6 | Treino e sensibilização interna: SINP |
| A 4.7 | Testes de aceitação de serviços |
| A 4.9 | Mecanismos de engodo |
| A 4.10 | Gestão de mudança e atualizações |
| A 5.1 | Nomear um CISO |
| A 5.2 | Estabelecer um serviço de gestão de vulnerabilidades |
| A 5.3 | Estabelecer e implementar um plano de auditorias |
| A 5.4 | Definir a missão, a comunidade servida e o portfólio de serviços do CSIRT |
| A 5.5 | Elaborar e fazer aprovar o plano e o orçamento para o CSIRT |
| A 5.6 | Montar e anunciar o CSIRT |
| A 5.7 | Estabelecer um sistema de gestão de Crise |
| A 5.8 | Afiliação nas comunidades nacionais e internacionais de CSIRT |
| A 5.9 | Participação num exercício nacional de cibersegurança |

## Anexo II – Sumário de capacidades (por fase)

| | CAPACIDADES |
|---|---|
| Fase I | Coopere com o CNCS numa base sistemática e tenha definido um ponto de contacto |
| | Tenha a noção dos principais ativos da organização |
| | Disponha de bases normativas internas para a proteção destes ativos críticos e da segurança de informação interna como um todo |
| Fase II | Intensifique o nível de cooperação com o CNCS com o estabelecimento de comunicações a nível operacional |
| | Proteja o perímetro da sua rede |
| | Disponha de informação de registo e fluxos de tráfego que permitem uma deteção atempada de ameaças, bem como o diagnóstico a posteriori do comportamento dos sistemas internos perante um evento de segurança |
| | Faça uma apropriada gestão e inventariação de ativos de informação internos, complementada com esquemas ou mapas da Rede |
| | Previna permanente os Riscos de inconformidade com a Lei e normativos ou certificações aplicáveis |
| | Disponha de resiliência ao nível da disponibilidade e integridade de informação, através da criação e manutenção de procedimento de backup e restore |
| | Acautele a formação dos recursos humanos internos de acordo com um mapa de competências |
| Fase III | Assegure a integridade e nível de segurança de sistemas aplicacionais internos |
| | Gira centralmente os equipamentos que suportam ativos de informação de forma eficiente |
| | Garanta a bom funcionamento dos equipamentos de suporte à infraestrutura de Rede |
| | Controle e centralize de forma eficaz a informação de eventos de segurança provenientes dos vários dispositivos e equipamentos de suporte à infraestrutura TIC num sistema SIEM |
| | Tenha equipas internas encarregadas da segurança de informação com formação nos domínios especializados da cibersegurança |
| Fase IV | Gira eficientemente os processos operacionais de segurança interna através da constituição formal de procedimentos |
| | Integre as políticas e normativos definidos em fases anteriores apropriadamente dentro de um quadro de gestão |

| | |
|---|---|
| | Garanta a manutenção da aplicação da metodologia de gestão de risco previamente definida |
| | Gira apropriadamente processos de mudança, incluindo a aplicação de patches e atualizações de segurança regulares |
| | Abranja a segurança de dispositivos móveis no quadro das medidas tecnológicas e processuais |
| | Condicione a entrada em produção de sistemas mediante a aplicação de testes de segurança e consequente aceitação por parte de uma equipa especializada |
| | Disponha de colaboradores sensibilizados nas áreas gerais de cibersegurança que tocam o desempenho das respetivas funções profissionais |
| | Disponha de hierarquias sensibilizadas para a importância da manutenção de um elevado nível de preparação e defesa ao nível da cibersegurança |
| Fase V | Disponha de um responsável máximo pela segurança de informação (CISO) |
| | Assegure a eficaz gestão de incidentes e vulnerabilidades, através da criação de uma equipa especializada (CSIRT) |
| | Conte com um sistema de gestão de crise nos processos internos |

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

outubro 2019

# Obrigado.