DESPACHO (PR) N.º 140 /2024

Assunto: Discussão Pública da proposta de Regulamento de Cibersegurança, Segurança de Informação, Privacidade e Proteção de Dados Pessoais do Instituto Politécnico do Cávado e do Ave

Nos termos do n.º 2 e do n.º 3 do artigo 110.º da Lei n.º 62/2007 de 10 de setembro (RJIES), do nº 6 do artigo 80º dos Estatutos do IPCA homologados pelo Despacho Normativo nº 1-A/2019, publicado na 2ª série do diário da república de 14 de junho, alterado pelo Despacho Normativo 2/2022, publicado na 2ª série do diário da república de 25 de janeiro, e do artigo 101.º do Código do Procedimento Administrativo, declaro em fase de discussão pública a proposta de "Regulamento de Cibersegurança, Segurança de Informação, Privacidade e Proteção de Dados Pessoais do Instituto Politécnico do Cávado e do Ave" visando a sua apreciação através da recolha de sugestões feitas pelos interessados.

O acesso à proposta de regulamento é feito através do site do IPCA, www.ipca.pt, no link "Discussão Pública".

Os contributos e sugestões devem ser efetuados por escrito e remetidos, no prazo de trinta dias a contar desta data, para o seguinte endereço de correio eletrónico: gapresidencia@ipca.pt

Barcelos, 30 de outubro de 2024

A Presidente do IPCA

[Assinatura Qualificada] Maria José da Silva Fernandes

Assinado de forma digital por [Assinatura Qualificada] Maria José da Silva Fernandes
Dados: 2024.10.30 15:07:27 Z

Professora Doutora Maria José Fernandes

REGULAMENTO DE CIBERSEGURANÇA, SEGURANÇA DE INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DO IPCA

PREÂMBULO

Atualmente, as tecnologias de informação são um instrumento de uso generalizado e estão na base de sistemas complexos que apoiam uma variedade de atividades quotidianas, assumindo um papel cada vez mais influente e determinante na forma como a vida em sociedade se desenvolve, o que se reflete não só na esfera dos agentes económicos e das relações privadas, mas também no âmbito da atividade pública e das relações entre os cidadãos e a Administração Pública. O IPCA tem adotado a digitalização e a conectividade como características centrais num número cada vez maior de serviços e procedimentos.

No entanto, o recurso a novas soluções digitais acarreta inevitavelmente a necessidade premente de assegurar um elevado nível de segurança das redes e dos sistemas de informação que sustentam o uso dessas novas tecnologias, de forma a garantir que a sua utilização decorre num ambiente de confiança e protegido de ameaças que possam ter efeitos desestabilizadores de considerável alcance na vida em sociedade, especialmente em contextos de crise, que tendem a agravar a exploração de vulnerabilidades por parte de agentes de ameaça com motivações diversas.

Neste contexto, a Lei n.º 46/2018, de 13 de agosto, veio estabelecer o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Esse regime foi, entretanto, objeto de regulamentação pelo Decreto-Lei n.º 65/2021, de 30 de julho, que definiu um conjunto de requisitos e obrigações em matéria de segurança do ciberespaço que devem ser cumpridas, designadamente, pela Administração Pública, incluindo as instituições de ensino superior.

Assim, verifica-se a necessidade de se proceder à regulamentação interna das disposições legais, com vista a estabelecer os princípios norteadores da atuação do IPCA em matéria de segurança do ciberespaço, definir a respetiva estrutura de segurança do ciberespaço e determinar as regras de segurança das redes e dos sistemas de informação e de notificação de incidentes que afetem a segurança dos mesmos, garantindo assim o integral e efetivo cumprimento dos requisitos e obrigações legais nesta matéria.

Capítulo I

Disposições Gerais da Segurança da Informação

Artigo 1.º

Objeto e âmbito de aplicação

1) O presente regulamento tem como objetivo principal estabelecer as diretrizes abrangentes para Cibersegurança, Segurança de Informação, Privacidade e Proteção de Dados Pessoais no IPCA, com os seguintes propósitos:
    a) Manter a confiança de colaboradores, parceiros, discentes e todas as partes interessadas do IPCA, assegurando a proteção dos dados sob sua responsabilidade;
    b) Salvaguardar os ativos de informação contra uso, divulgação, alteração ou destruição não autorizados, alinhando as medidas de segurança com sua importância e sensibilidade;
    c) Garantir a efetiva capacidade de resposta a incidentes de segurança da informação, minimizando o impacto financeiro, reputacional e operacional associado;
    d) Cumprir todas as obrigações legais e regulamentares relativas à Segurança da Informação, em consonância com as atividades do IPCA.
2) Este regulamento define os princípios orientadores da atuação do IPCA em matéria de Segurança de Informação, Cibersegurança e Proteção da Privacidade, bem como estabelece

a estrutura de Segurança de Informação. Além disso, determina as regras aplicáveis à segurança das redes e sistemas de informação, bem como os procedimentos de notificação de incidentes que afetem a segurança desses sistemas, com o intuito de cumprir os requisitos e obrigações legais relacionados com a Segurança de Informação.

3) As disposições contidas neste regulamento aplicam-se a todas as unidades orgânicas, bem como a outras unidades e serviços do IPCA que façam uso das redes de dados e sistemas de informação.
4) A utilização das redes de dados e sistemas de informação do IPCA por entidades externas deve estar em conformidade com os requisitos e obrigações estabelecidos neste regulamento.

Artigo 2.º

Definições

Para a finalidade deste Regulamento entende-se por:

a) **Ativo de Informação**: Qualquer dado, informação, sistema, equipamento ou recurso que seja valioso para o IPCA e que necessita ser protegido.
b) **Ativo (Informático):** Todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pelo IPCA, que suportam, direta ou indiretamente, um ou mais serviços;
c) **Ativo Privado**: Ativo apenas acessível internamente, seja diretamente ao equipamento ou a partir de redes informáticas internas ao IPCA;
d) **Ativo Público**: Qualquer ativo acessível diretamente através da internet;
e) **Autoridade de controlo**: uma autoridade pública independente criada por um Estado-Membro no âmbito a que se destina.
f) **Classificação da Informação**: Atribuição de níveis de sensibilidade à informação com base no seu valor, criticidade e sensibilidade, determinando o acesso e os controlos de segurança adequados.

g) **CNCS** (Centro Nacional de Cibersegurança): Instituição nacional que promove a utilização do ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurança nacional e da cooperação internacional.

h) **Controlos de Segurança**: Procedimentos, tecnologias e práticas implementadas para proteger a informação e reduzir os riscos de incidentes de segurança.

i) **CSIRT** (Computer Security Incident Response Team): Equipa de peritos cuja função é dar resposta a incidentes de segurança informática e gerir de incidentes.

j) **Dados pessoais**: informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

k) **Incidente de Segurança da Informação**: Qualquer evento que representa uma violação, ameaça ou comprometimento da segurança da informação ou dos ativos do IPCA.

l) **Informação**: Por Informação entende-se todo e qualquer dado independentemente da natureza, incluindo dados relativos à atividade do IPCA, ou de terceiros com quem se relacione, que a organização coloque à disposição dos seus trabalhadores e de entidades externas, ou que estes possam vir a ter conhecimento ou acesso no exercício das suas funções. A Informação deve ser considerada independentemente do seu suporte ou via de transmissão.

m) **Função**: é a denominação de um conjunto de tarefas e responsabilidades para as quais a estrutura de responsabilização foi prevista no organograma do IPCA e que é atribuída a um trabalhador ou entidade (gabinete, direção, divisão ou serviço).

n) **Redes de Dados**: Conjunto de dois ou mais dispositivos eletrónicos de computação (módulos processadores ou nós de rede) interligados por um sistema de comunicação digital (ligação de dados) que utilizam um conjunto de regras (protocolos de rede) para partilharem entre si informação, serviços e recursos físicos e lógicos;

o) **Responsável pela Segurança da Informação**: Pessoa ou equipa designada com a responsabilidade de supervisionar e implementar as políticas e controlos de segurança da informação.

p) **Segurança da Informação**: Conjunto de medidas e práticas destinadas a proteger a confidencialidade, integridade e disponibilidade da informação, bem como os sistemas que a processam e armazenam.

q) **Sistema de Informação**: Qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações eletrónicas que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;

r) **Titular dos Dados**: é uma pessoa singular identificada ou identificável, nos termos do artigo 4.º, n.º 1, 1) do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados, "RGPD").

s) **TLP (Traffic Light Protocol)**: Protocolo que providencia um esquema fácil para indicar quando (proteção) e como (divulgação) a informação pode ser partilhada com a comunidade de cibersegurança a nível nacional e internacional, o qual adota um esquema de cores (semáforo) para indicar os diferentes níveis de sensibilidade e ações expectáveis, que devem ser obrigatoriamente respeitadas no manuseamento da informação;

t) **Tratamento de Dados Pessoais**: uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

u) **Tratamento de Incidentes**: Todos os procedimentos de apoio à deteção, análise, contenção e resposta a um incidente.

v) **Violação de dados pessoais**: uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Artigo 3º

Princípios Fundamentais da Segurança da Informação e Proteção de Dados

Os princípios fundamentais, conceitos essenciais e inegociáveis, pelos quais o IPCA se rege são:

a) **Confidencialidade** – O IPCA compromete-se a garantir a proteção da informação contra o acesso não autorizado.

b) **Integridade** – O IPCA compromete-se a garantir a correção, precisão, confiança e completude da informação e dos seus métodos de utilização, processamento e transporte.

c) **Disponibilidade** – Garantia do acesso à informação de pessoas ou processos autorizados, de acordo com os requisitos identificados pelo IPCA.

d) **Privacidade** – O IPCA garante que as informações e dados pessoais são tratados de acordo com as leis e regulamentos aplicáveis, evitando a sua divulgação ou uso indevido.

e) **Não repúdio** – O IPCA garante através dos devidos procedimentos tecnológicos que, nas suas infraestruturas tecnológicas, nenhuma pessoa ou entidade poderá negar a autenticidade de uma comunicação, transação ou uma ação realizada.

Artigo 4.º

Princípios Gerais

O IPCA estabelece os seguintes princípios gerais para garantir a Cibersegurança, Segurança de Informação, Privacidade e Proteção de Dados Pessoais:

a) **Responsabilidade Institucional**: O IPCA assume a responsabilidade de desenvolver e implementar políticas, procedimentos e estratégias de Cibersegurança, Segurança de Informação, Privacidade e Proteção de Dados Pessoais, com objetivo de promover uma cultura de segurança, salvaguardar a sua infraestrutura tecnológica e promover a privacidade e proteção dos dados aos quais tem acesso da sua comunidade.

b) **Participação da comunidade académica**: Todos os membros da comunidade académica, incluindo docentes, discentes, pessoal não-docente e restantes parceiros, são incentivados a participar ativamente na adoção de comportamentos preventivos e na adoção de boas práticas no âmbito deste regulamento.

c) **Prevenção e Deteção de Incidentes de Cibersegurança**: São adotadas medidas preventivas e implementadas tecnologias de prevenção e deteção de incidentes de Cibersegurança, com o objetivo de identificar e mitigar potenciais riscos à segurança da informação e de violação de dados pessoais e privacidade.

d) **Transparência e privacidade**: O IPCA mantém uma política de privacidade clara e transparente, comunicando de forma adequada a recolha, tratamento e finalidades dos dados pessoais dos seus colaboradores, discentes e parceiros. É obtido o consentimento informado dos titulares dos dados pessoais, sempre que aplicável, para o tratamento desses dados garantindo a conformidade com o Regulamento Geral de Proteção de Dados e restantes leis em vigor nomeadamente no que diz respeito à licitude, proporcionalidade, minimização e observância pela necessidade do conhecer.

e) **Adequação**: O IPCA acata as instruções técnicas de cibersegurança emitidas pelas estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime, ciberterrorismo e proteção de dados pessoais e age em conformidade com as mesmas, bem como adequa as medidas técnicas e organizativas ao nível nacional de alerta, sem prejuízo de poder emitir instruções internas adicionais que não se sobreponham ou sejam contrárias àquelas;

f) **Cooperação**: O IPCA colabora e atua em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime, ciberterrorismo e proteção de dados pessoais, devendo comunicar às autoridades

competentes, no mais curto prazo possível, os factos de que tenha conhecimento relativos a incidentes de segurança informática, identificados pelo próprio IPCA ou notificados pelas entidades legalmente competentes;

g) **Classificação da informação**: O IPCA respeita o protocolo TLP para a classificação da informação no âmbito da comunicação de incidentes de segurança;

h) **Colaboração para a partilha de recursos**: O IPCA pode estabelecer formas de colaboração com as entidades previstas nas alíneas a) a d) do n.º 1 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, com vista ao cumprimento das obrigações em matéria de requisitos de segurança e de notificação de incidentes, numa lógica de partilha de recursos, desde que seja assegurada a efetiva operacionalização das mesmas em cada entidade e sem prejuízo da responsabilização de cada entidade individualmente considerada pelo incumprimento daquelas obrigações;

i) **Colaboração interna**: Com vista ao cumprimento das obrigações previstas na lei e no presente Regulamento, as unidades orgânicas e outras unidades e serviços centrais do IPCA abrangidas pelo n.º 2 do artigo 1.º colaboram e atuam em articulação e estreita cooperação com o responsável de segurança, com o ponto de contacto permanente e com o serviço responsável pela cibersegurança do IPCA.

Artigo 5.º

Princípios Transversais

Os princípios gerais são completados pelos princípios transversais que contribuem para a melhoria continua da Segurança da Informação:

a) **Acessos Lógicos** – Acesso individual exclusivo aos ativos de informação necessários ao desempenho das funções;

b) **Segregação de funções** – Separação real e permanente entre a autorização e a execução de cada processo, no âmbito da segurança de informação, por forma a garantir que ninguém, individualmente, tem controlo exclusivo sobre um ativo de informação ou processo associado;

c) **Proporcionalidade –** A aplicação dos princípios gerais de segurança da informação é proporcional ao risco do ativo de informação;

d) **Resiliência –** A proteção e monitorização sistemas de informação deve garantir a robustez de todos os elementos envolvidos, pessoas, processos e tecnologia;

e) **Manutenção da confiança** – O nível de proteção deve ser consistente em todas as componentes dos ativos de Informação.

Capítulo II

Organização e Responsabilidades em Cibersegurança, Segurança de Informação, Privacidade e Proteção de Dados Pessoais

Artigo 6.º

Privacidade e Proteção de Dados Pessoais

1) A privacidade e a proteção de dados pessoais são prioritárias em todas as operações realizadas pelo IPCA, que mantém um compromisso constante com a conformidade legal e o respeito escrupuloso pela proteção de dados e privacidade dos seus titulares.
2) Com base na Política de Privacidade do IPCA e nas disposições do Regulamento Geral sobre a Proteção de Dados, o IPCA adota um compromisso abrangente, que contempla várias dimensões críticas. Estas dimensões incluem, mas não se limitam à adoção de práticas de segurança aplicáveis à recolha e tratamento de dados pessoais, à conservação de dados pessoais, à partilha de dados com terceiros, ao estabelecimento de políticas de acesso e controlo dos dados pessoais, bem como a utilização de cookies e outras tecnologias nos termos legalmente admissíveis.
3) Para assegurar o cumprimento desses termos e requisitos em vigor neste domínio, o IPCA estabeleceu a colaboração com um Encarregado de Proteção de Dados (EPD/DPO) devidamente designado.

4) O EPD/DPO tem a missão de, entre outras atividades, analisar, informar e aconselhar de forma independente, sobre as obrigações legais relacionadas com o Regulamento Geral sobre a Proteção de Dados, bem como sobre a aplicabilidade e manutenção da Política de Privacidade da organização.
5) O EPD/DPO cumpre ainda a função de ponto de contacto do IPCA com a Autoridade de Controlo (Comissão Nacional de Proteção de Dados), com os Titulares de Dados e, ainda, é responsável pela manutenção de um registo atualizado das atividades de tratamento do IPCA, medidas de segurança existentes e avaliações de impacto necessárias.

Artigo 7.º

Administração de Segurança da Informação

1) Nos termos do presente regulamento é criada a Administração de Segurança da Informação do IPCA, doravante ASI, que tem como missão gerir a segurança da informação cuja gestão visa apropriar-se adequadamente dos riscos correspondentes para assegurar a confidencialidade, integridade e disponibilidade da informação.
2) A ASI é responsável pela criação do Modelo de Administração de Segurança da Informação.
3) O Modelo identifica as Funções da ASI nos diversos processos da Gestão de Segurança da Informação
4) A estrutura da ASI, compreende:
   a) No nível estratégico - o Presidente do IPCA, o Conselho de Gestão e o Comité de Segurança da Informação;
   b) No nível tático/técnico, - o CISO (Chief Information Security Officer) e o Administrador de Segurança da Informação;
   c) No nível operacional - a Equipa de Segurança da Informação.

Artigo 8.º

Presidente do IPCA

1) O Presidente do IPCA desempenha um papel fundamental na gestão direta da segurança da informação, contando com o apoio de especialistas em segurança da informação e de uma equipa de secretariado, todos designados pela própria Presidência.
2) O Presidente do IPCA tem a responsabilidade de aprovar assuntos e documentos relacionados com a gestão de segurança de informação.
3) Periodicamente, o Presidente do IPCA revê, avalia e, quando necessário, redefine as responsabilidades e tarefas atribuídas ao ASI-CISO (Administrador de Segurança da Informação), seguindo os referenciais associados ao cargo estabelecidos no "Modelo de Administração de Segurança da Informação".
4) É de responsabilidade do Presidente do IPCA nomear o responsável de segurança, conforme previsto no Decreto-Lei n.º 65/2021, designar os pontos de contacto permanente e efetuar a devida notificação ao CNCS.

Artigo 9.º

Comité de Segurança da Informação (CSI)

1) O Comitê de Segurança da Informação (CSI) tem a responsabilidade de estabelecer diretrizes essenciais para alcançar os objetivos de segurança da informação, alinhados com os objetivos do IPCA.
2) O CSI é presidido pelo Presidente do IPCA ou em quem ele delegar, que nomeia seus membros, incluindo o Administrador de Segurança da Informação (ASI-CISO), o Data Protection Officer (DPO) e representantes de várias áreas.
3) O CSI supervisiona o cumprimento das medidas de segurança da informação por meio de revisões periódicas, análise de indicadores e gestão de um programa de auditorias internas para verificar a eficácia dos controlos de segurança da informação.

4) O CSI reúne-se e anualmente para avaliação e aprovação de um plano de atividades e investimentos para a ASI, bem como das políticas da Segurança da Informação e Cibersegurança.
5) O CSI reúne-se extraordinariamente por iniciativa do ASI-CISO ou da Presidência.

Artigo 10.º

Administrador de Segurança da Informação – CISO

1) O ASI-CISO, nomeado pelo Presidente do IPCA, é o responsável pela efetiva implementação, operacionalização, manutenção e melhoria da Gestão de Segurança da Informação e dos seus controlos. Possui autoridade e responsabilidades definidas para direcionar as políticas de segurança de informação e alocar os recursos necessários para alcançar o desempenho esperado.
2) O ASI-CISO coordena a Equipa de Segurança da Informação e supervisiona a avaliação e tratamento de riscos de segurança da informação.
3) O ASI-CISO é responsável pela elaboração do Plano de Gestão da Segurança da Informação, Programa de Auditorias, Plano de Oportunidades de Melhoria.
4) O ASI-CISO deve participar anualmente na revisão pela gestão nas vertentes tática e operacional, de acordo com as diretrizes definidas no referido Modelo.

Artigo 11.º

Equipa de Segurança da Informação

1) A Equipa de Segurança avalia riscos, implementa controlos e comunica políticas de segurança.
   a) Avalia riscos, planeia e controla controlos de segurança em conjunto com os Donos dos Processos, Risco e ativos correspondentes.
   b) Comunica políticas de segurança aos trabalhadores e entidades externas.
2) Os membros da Equipa são propostos pelo ASI-CISO e aprovados pelo Presidente do IPCA.

Artigo 12.º

Trabalhadores do IPCA

1) Os trabalhadores do IPCA estão sujeitos ao cumprimento das políticas, processos e procedimentos aplicáveis, definidos pela Equipa de Segurança da Informação.
2) Não é permitida a utilização de informação e/ou de sistemas e tecnologias de informação do IPCA para fins distintos daqueles para os quais foram autorizados pelo IPCA.
3) Os trabalhadores e os prestadores de serviço que utilizam os serviços e os sistemas de informação do IPCA quando detetam qualquer ponto fraco de segurança da informação, observado ou suspeito, nos sistemas ou serviços devem reportar o Incidente de Segurança de Informação de acordo com o processo documentado de Gestão de Incidentes de Segurança de Informação.

Artigo 13.º

Modelo de Administração de Segurança de Informação

1) O Modelo de Administração de Segurança de Informação (MASI) é um documento que pretende estabelecer a Organização de Segurança da Informação do IPCA, designada como a estrutura funcional da gestão da Segurança da Informação (GSI). As funções são caracterizadas pelas suas responsabilidades na GSI e nos papéis de processos aplicáveis, assim como a relação da Organização de SI com outros processos que suportam as atividades de planeamento, operação, manutenção e melhoria contínua do sistema.
2) O MASI é aprovado pelo Comité de Segurança.
3) O âmbito de atuação da ASI é regido pelo quadro de funcionamento estabelecido no MASI, que salvaguarda os seguintes princípios:
    a) Comprometimento contínuo com a segurança da informação;
    b) Garantia e reforço da conformidade com a regulamentação e exigências legais em vigor;

c) Confidencialidade, integridade e disponibilidade da informação;

d) Estabelecimento de um padrão de qualidade consistente com a dimensão e importância da organização.

Capítulo III

Disposições Gerais da Legislação Aplicável

Artigo 14.º

Ponto de contacto permanente

1) A Presidente do IPCA deverá indicar, pelo menos, um ponto de contacto permanente, de modo a assegurar os fluxos de informação de nível operacional e técnico com o CNCS, nomeadamente:

a) A obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto relevante ou substancial submetida pela mesma ou outra entidade;

b) A obtenção e atualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial;

c) A partilha de informação quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da segurança do ciberespaço, bem como de planos no âmbito do planeamento civil de emergência do ciberespaço ou dos planos de segurança das infraestruturas críticas nacionais ou europeias;

d) A operacionalização dos procedimentos fixados no âmbito de um plano de emergência de proteção civil quando tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência do ciberespaço;

e) A receção das instruções técnicas emitidas ao abrigo do disposto no n.º 5 do artigo 7.º e no artigo 18.º do Regime Jurídico da Segurança do Ciberespaço (Lei n.º 46/2018, de 13 de agosto);

f) A operacionalização dos procedimentos fixados no âmbito dos planos de segurança previstos no artigo 7.º

2) O IPCA deve assegurar a função de ponto de contacto permanente com uma disponibilidade contínua de 24 horas por dia e de sete dias por semana, limitada a períodos de ativação, iniciados e terminados mediante comunicação do CNCS.

3) O IPCA deve indicar ao CNCS, no prazo de 20 dias úteis a contar do início da respetiva atividade, a pessoa ou pessoas responsáveis por assegurar as funções de ponto de contacto permanente, bem como os respetivos meios de contacto principal e alternativos.

Artigo 15.º

Responsável de segurança

1) De acordo com o número 3 do Artigo 9º, a Presidente do IPCA terá a responsabilidade de nomear o responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do Decreto-Lei n.º 65/2021.

2) A pessoa designada para as funções de responsável de segurança deve ser indicada pelo IPCA ao CNCS, no prazo de 20 dias úteis a contar do início da respetiva atividade.

3) É da responsabilidade do responsável de segurança do IPCA a gestão do conjunto de medidas implementadas relacionadas com os requisitos de segurança e a notificação de incidentes, conforme estabelecido pela lei, pelo presente Regulamento, segundo as políticas aprovadas pelo Comité de Segurança e em estreita colaboração com o ASI-CISO.

4) O IPCA deve comunicar imediatamente ao CNCS a substituição do responsável de segurança.

Artigo 16.º

Inventário de ativos

1) O IPCA deve elaborar e manter atualizado um inventário de todos os ativos essenciais para a prestação dos respetivos serviços, devendo o mesmo ser assinado pelo responsável de segurança.
2) No inventário de ativos deve constar, para cada ativo, a informação definida em instruções técnicas emitidas pelo CNCS. regulamentação complementar em vigor, nomeadamente em instruções técnicas emitidas pelo CNCS e transpostas para a política de gestão de ativos e as demais políticas referidas na mesma.
3) O IPCA comunicar ao CNCS a lista dos ativos constantes do inventário, com a informação que venha a ser determinada nos termos do número anterior, com a seguinte periodicidade:
   a) Na sua versão inicial, no prazo de 20 dias úteis a contar da data de início de atividade;
   b) Numa versão atualizada, anualmente, a ser entregue em conjunto com o relatório anual a que se refere o artigo 8.º do Decreto-Lei n.º 65/2021.

Artigo 17.º

Plano de segurança

1) O IPCA deve elaborar e manter atualizado um plano de segurança, devidamente documentado e assinado pelo responsável de segurança, que contenha:
   a) A política de segurança, incluindo a descrição das medidas organizativas e a formação de recursos humanos;
   b) A descrição de todas as medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes;
   c) A identificação do responsável de segurança;
   d) A identificação do ponto de contacto permanente.

2) Para efeitos do cumprimento do disposto no número anterior, os operadores de infraestruturas críticas podem utilizar o plano previsto no artigo 10.º do Decreto-Lei n.º 62/2011, de 9 de maio, desde que o mesmo inclua medidas relativas à segurança das redes e da informação.

Artigo 18.º

Relatório Anual

1) O IPCA elaborar um relatório anual que, em relação ao ano civil a que se reporta, contenha os seguintes elementos:
   a) Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e dos serviços de informação;
   b) Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes;
   c) Análise agregada dos incidentes de segurança com impacto relevante ou substancial, com informação sobre:
      i) Número de utilizadores afetados pela perturbação do serviço;
      ii) Duração dos incidentes;
      iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
   d) Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação;
   e) Problemas identificados e medidas implementadas na sequência dos incidentes;
   f) Qualquer outra informação relevante.
2) O IPCA deve remeter o relatório anual ao CNCS, devidamente assinado pelo responsável de segurança, nos seguintes termos:
   a) Relativamente ao primeiro relatório anual:

i) Até ao último dia útil do mês de janeiro do ano civil seguinte ao primeiro ano civil de atividade, quando esta tenha tido início no primeiro semestre;

ii) Até ao último dia útil do mês de janeiro do segundo ano civil seguinte ao primeiro ano civil de atividade, quando esta tenha tido início no segundo semestre;

b) Relativamente aos relatórios subsequentes anuais, até ao último dia útil do mês de janeiro do ano civil seguinte aos quais os mesmos se reportam.

3) Para efeitos do disposto na subalínea ii) da alínea a) do número anterior, o relatório anual deve abranger todo o período entre a data de início de atividade e o final do ano civil anterior.

4) Para efeitos do disposto no presente artigo, o CNCS pode definir o formato em que a informação deve ser apresentada.

Capítulo IV

Segurança da Informação, Privacidade e Proteção de Dados

Artigo 19.º

Medidas para cumprimento dos requisitos de segurança

1) O IPCA, como entidade referida na alínea a) do n.º 2 do artigo 1.º do Decreto-Lei n.º 65/2021 deve cumprir as medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, devendo, para o efeito, realizar uma análise dos riscos de acordo com o disposto no artigo seguinte.

2) As medidas referidas no número anterior devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes, através da utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.

Artigo 20.º

Análise dos riscos e implementação dos requisitos de segurança

1) O ASI-CISO é responsável pela realização anual de uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e também em relação aos ativos que garantam a prestação dos serviços essenciais, nos seguintes termos:
   a) Análise dos riscos de âmbito global, com a seguinte periodicidade:
      i) Pelo menos uma vez por ano;
      ii) Após a notificação, por parte do CNCS, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que implique uma elevada probabilidade de ocorrência de um incidente com impacto relevante, dentro do prazo fixado pelo CNCS;
   b) Análise dos riscos de âmbito parcial, com a seguinte periodicidade:
      i) Durante o planeamento e preparação da introdução de uma alteração ao ativo ou ativos, em relação ao ativo ou ativos envolvidos;
      ii) Após a ocorrência de um incidente com impacto relevante ou outra situação extraordinária, em relação aos ativos afetados;
      iii) Após a notificação, por parte do CNCS, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que impliquem uma elevada probabilidade de ocorrência de um incidente com impacto relevante, dentro do prazo fixado pelo CNCS;
2) O ASI-CISO deve garantir a documentação, preparação, execução e a apresentação dos resultados da análise dos riscos;
3) A análise do risco deve abranger para cada ativo:
   a) A identificação das ameaças, internas ou externas, intencionais ou não intencionais, incluindo, nomeadamente:
      i) Falha de sistema;
      ii) Fenómeno natural;
      iii) Erro humano;

iv) Ataque malicioso;

v) Falha no fornecimento de bens ou serviços por terceiro;

b) A caracterização do impacto e da probabilidade da ocorrência das ameaças identificadas na alínea anterior.

4) A análise dos riscos deve ter em consideração:

a) O histórico de situações extraordinárias ocorridas;

b) O histórico de incidentes e, em especial, de incidentes com impacto relevante;

c) O número de utilizadores afetados pelos incidentes;

d) O tipo de dados e de titulares de dados afetados;

e) A duração dos incidentes;

f) A distribuição geográfica, no que se refere à zona afetada pelos incidentes;

g) As dependências intersetoriais para efeitos da prestação dos serviços, incluindo os constantes do anexo ao Regime Jurídico da Segurança do Ciberespaço e o setor das comunicações eletrónicas.

5) A análise dos riscos deve ainda ter em consideração a avaliação integrada dos riscos para a segurança das redes e dos sistemas de informação a nível nacional, europeu e internacional, publicada anualmente ou notificada ao IPCA pelo CNCS.

6) Na sequência de cada análise dos riscos, o IPCA deve adotar as medidas técnicas e organizativas adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, e que resultem, nomeadamente:

a) De normativo complementar setorial aprovado pelo CNCS, sem prejuízo da aplicação de outro normativo nacional e da União Europeia em matéria da segurança das redes e dos sistemas de informação;

b) Do Quadro Nacional de Referência de Cibersegurança, e respetivas disposições complementares, elaborado pelo CNCS, na ausência ou em complemento do normativo setorial previsto na alínea anterior.

7) Os riscos para a segurança das redes e dos sistemas de informação caracterizados como residuais devem ser tratados pelo IPCA nos termos do número anterior.

8) O IPCA deve rever e, se necessário, atualizar o seu plano de segurança, nos termos previstos no artigo 7.º, em função da evolução do contexto de atuação e da ocorrência de incidentes.
9) As medidas a adotar ao abrigo do disposto no n.º 6 do presente artigo devem permitir:
   a) A prevenção, a gestão e a redução dos riscos;
   b) O reforço da robustez e da resiliência dos ativos, incluindo a respetiva proteção contra as ameaças identificadas e a respetiva recuperação ou redundância, de forma a assegurar um rápido restabelecimento do funcionamento das redes e dos sistemas de informação;
   c) Uma resposta eficaz a incidentes, a ameaças ou a vulnerabilidades.
10) Para efeitos do disposto no presente artigo, o CNCS pode emitir instruções técnicas com vista a uma harmonização da matriz de risco a adotar pelo IPCA.

Capítulo V

Notificações de incidentes

Artigo 21.º

Obrigações de notificação

1) O IPCA notifica o CNCS da ocorrência de incidentes com impacto relevante ou substancial nos termos, respetivamente, dos artigos 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço.
2) O IPCA deve implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à notificação de incidentes com impacto relevante ou substancial.
3) O IPCA deve, perante qualquer incidente detetado ou a este comunicado pelos seus clientes, utilizadores ou outras entidades, atender aos parâmetros previstos, respetivamente, no n.º 4 do artigo 15.º, no n.º 4 do artigo 17.º e no n.º 4 do artigo 19.º do Regime Jurídico da Segurança do Ciberespaço, bem como aos constantes dos normativos complementares setoriais aplicáveis, para classificar os incidentes como tendo impacto relevante ou substancial.

4) Sempre que um ocorra um Incidente de Segurança da Informação que envolva dados pessoais, a Equipa de Segurança da Informação deve comunicar, imediatamente, o mesmo ao EPD/DPO, para que este possa analisar se se trata de uma violação de dados pessoais nos termos do Regulamento Geral sobre a Proteção de Dados e proceder em conformidade com a notificação do mesmo à Autoridade Supervisora e Titulares de Dados, conforme aplicável.

Artigo 22.º

Tipos de notificações

Por cada incidente que deva ser objeto de notificação ao abrigo do disposto no artigo anterior, o IPCA contactar o CNCS, seguindo todos os procedimentos desde a notificação inicial à notificação final, em total cumprimento com o Decreto-Lei n.º 65/2021, nos termos dos artigos 12º a 15º.

Artigo 23.º

Taxonomia de incidentes e de efeitos

Para efeitos do disposto nos artigos 13.º a 15.º, do Decreto-Lei n.º 65/2021, os incidentes são categorizados pelo IPCA tendo em conta o documento de classificação da Rede CSIRT referido no procedimento de classificação e comunicação de incidentes de segurança da informação, bem como o disposto no artigo 16º do referido Decreto de Lei.

Artigo 24.º

Disposições complementares

1) O CNCS presta à entidade notificante, IPCA, as informações relevantes relativas ao processamento do incidente notificado, nomeadamente informações que possam contribuir para o tratamento eficaz do incidente.

2) O IPCA deve dar resposta a qualquer pedido de informação adicional por parte do CNCS sobre os incidentes reportados.
3) O IPCA pode optar por enviar ao CNCS qualquer campo de informação antes do final dos prazos fixados para o efeito, desde que disponham de informação fiável para o fazer.
4) Sem prejuízo do disposto no presente capítulo, o IPCA deve seguir o formato e o procedimento de notificação de incidentes definido nos normativos complementares setoriais aplicáveis.

CAPÍTULO VI

Disposições complementares e finais

Artigo 25.º

Comunicações

1) As comunicações entre o IPCA e o CNCS, incluindo as notificações de incidentes, devem seguir o formato e o procedimento definido em regulamentação complementar.
2) Na ausência de regulamentação complementar, todas as comunicações dirigidas ao CNCS no âmbito do Decreto-Lei n.º 65/2021, bem como o envio de informação, devem ser realizadas por meios eletrónicos e nos prazos definidos no referido decreto de lei.
3) O CNCS mantém e gere a informação em matéria de segurança e integridade num sistema de informação seguro, em conformidade com as disposições respeitantes à segurança de matérias classificadas no âmbito nacional e no âmbito das organizações internacionais de que Portugal é parte.
4) O acesso aos sistemas eletrónicos e sítios de Internet para tratamento das notificações previstas no presente decreto-lei deve ser efetuado preferencialmente com recurso a sistema de identificação eletrónico com nível de garantia «elevado», nos termos definidos pelos artigos 8.º e 9.º do Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança, designadamente através do Cartão de Cidadão e da Chave Móvel Digital.

5) Nos casos em que o IPCA não tenha temporariamente capacidade operacional para assegurar a comunicação prevista nos artigos 2 e 3 do Decreto-de-lei 65/2021, ou nos casos em que o sítio na Internet do CNCS esteja indisponível, em resultado do incidente ou por outro motivo de natureza eminentemente técnica devidamente justificado, a notificação pode ser efetuada, a título excecional, através de correio eletrónico ou telefonicamente, de acordo com instruções técnicas a emitir pelo CNCS.

Artigo 26.º

Medidas excecionais de segurança

1) Em caso de situações que possam afetar a segurança e o normal funcionamento das redes e dos sistemas de informação, a Equipa de Segurança da Informação do IPCA pode adotar as medidas excecionais que se revelem tecnicamente adequadas e proporcionais à mitigação e à resolução do incidente, sem prejuízo da imediata comunicação fundamentada das mesmas ao responsável de segurança, ao ponto de contacto permanente e ao ASI-CISO do IPCA.
2) As medidas excecionais de segurança a aplicar podem consistir, nomeadamente:
    a. Na limitação de acesso ao ciberespaço do IPCA;
    b. Na restrição de acesso:
        i. A redes do IPCA;
        ii. À internet;
        iii. A sistemas do IPCA;
        iv. A sistemas externos.
3) A duração das medidas adotadas no âmbito do número anterior é determinada pelo ASI-CISO do IPCA e comunicada ao ponto de contacto permanente, ao responsável de segurança e à Equipa de Segurança da Informação do IPCA.

Artigo 27.º

Dúvidas de interpretação e casos omissos

As dúvidas suscitadas pela aplicação do presente Regulamento e os casos omissos são resolvidos por despacho da Presidente do IPCA, tendo em consideração a legislação em vigor, atenção a lei e as normas e regulamentos vigentes no IPCA, bem como as instruções técnicas emitidas pelo CNCS.

Artigo 28.º

Responsabilidade

1) As unidades orgânicas e outras unidades do IPCA abrangidas pelas n.ºs 2 e 3 do artigo 1.º poderão ser financeiramente responsáveis, perante o IPCA, pelo pagamento de coimas aplicadas ao IPCA no âmbito de processos de contraordenação que resultem do incumprimento, por parte daquelas unidades ou serviços, de qualquer obrigação prevista no presente Regulamento.
2) O disposto no número anterior não prejudica a responsabilização financeira e disciplinar individual pelo incumprimento das obrigações previstas no presente Regulamento, nos termos da lei geral.

Artigo 29.º

Revogação

1) Este regulamento substituirá qualquer regulamento anterior relacionado ao mesmo tema, excetuando as existentes e relacionadas, mas atinentes ao departamento de proteção de dados pessoais.
2) Com a entrada em vigor do presente regulamento, são revogadas todas as normas internas e regulamentos do IPCA que contrariem o nele disposto.

Artigo 30.º

Data de Entrada em Vigor

Este regulamento entrará em vigor no dia seguinte à sua publicação em Diário da República.