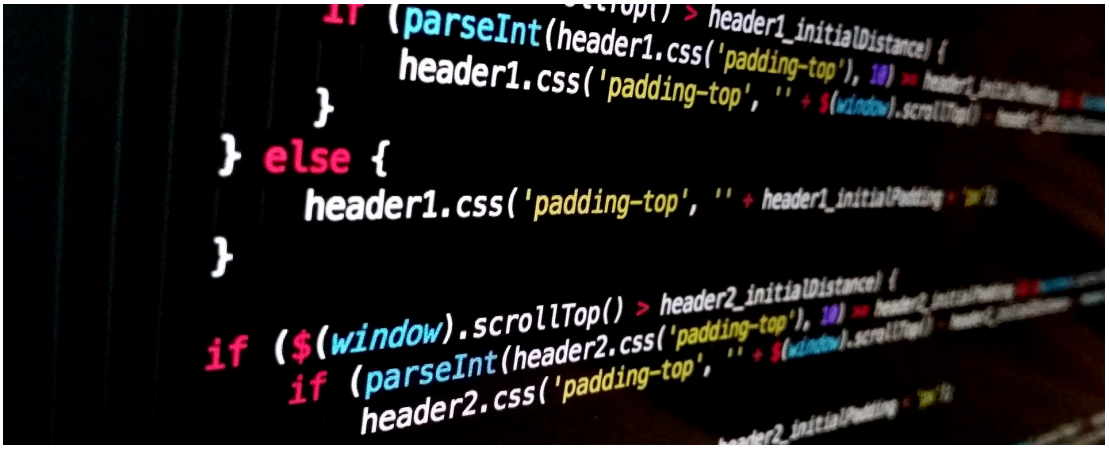
AMMOURA

INSIGHTS



MEDIDAS ORGANIZATIVAS E DE SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS: NOVAS DIRETRIZES DA CNPD

A **Comissão Nacional de Proteção da Dados** (CNPD) publicou, recentemente, a **Diretriz/2023/1** sobre **medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais**, em resposta aos múltiplos **ataques a sistemas de informação**, incluindo *phishing*, *malware* e *ransomware*, que ocorrem com crescente frequência, dimensão e complexidade, afetando, na sua grande maioria, dados pessoais.

> Entidades abrangidas

As medidas técnicas e organizativas devem ser adotadas, designadamente, pelo **responsável pelo tratamento de dados pessoais** e pelo **subcontratante**.

> Medidas técnicas e organizativas

As medidas técnicas e organizativas visam conferir ao tratamento de dados pessoais um nível **de segurança adequado ao risco**, incluindo a capacidade a **confidencialidade**, a **integridade**, a **disponibilidade** e a **resiliência** dos sistemas e serviços de tratamento.

Exemplos de medidas de segurança organizativas:

a) Documentar as **políticas de segurança**.

b) Definir **políticas de gestão de palavras-passe** seguras, incluindo requisitos de tamanho, composição, armazenamento e frequência de alteração das mesmas.

c) Criar **política de gestão dos utilizadores**, garantindo apenas o acesso aos dados necessários,

revendo as permissões dos vários perfis e desativando os perfis inativos.

d) Desenvolver **política interna** para resolver e documentar **violações de dados pessoais**.

e) Documentar e corrigir as **vulnerabilidades de segurança** detetadas sem demora.

f) Adotar **alarmística** de identificação de situações de acesso, tentativas ou utilização indevida.

g) Adotar procedimentos de análise para a **monitorização dos fluxos de tráfego** na rede.

h) Realizar **auditorias de segurança** e **avaliações de vulnerabilidade** sistemáticos.

i) Fomentar junto dos colaboradores uma **cultura de privacidade e segurança** da informação.

j) Avaliar e atualizar periodicamente as medidas de segurança internas.

Exemplos de medidas de segurança técnicas:

a) **Autenticação** — utilizar credenciais fortes, com palavras-passe longas, únicas, complexas, com números, símbolos, letras maiúsculas e minúsculas, sujeitas a frequentes alterações; aplicar a autenticação multifator.

b) **Infraestrutura e sistemas** — atualizar sistemas operativos de servidores, terminais, aplicações, e *firmware* dos equipamentos de rede; segmentar ou isolar os sistemas e as redes de dados; robustecer a segurança dos postos de trabalho e servidores, bloqueando o acesso a sítios suscetíveis de constituir risco para a segurança, redireccionamentos suspeitos através de motores de busca, e ficheiros e aplicações infetadas com *malware*; ativar e conservar os registos de auditoria *log*, validar os acessos por *IP* aos servidores que estão expostos ao público e configurar o protocolo de acessos remotos *RDP*.

c) **Ferramenta de correio eletrónico** — definir políticas e procedimentos internos sobre o envio de mensagens de correio eletrónico com dados pessoais; encriptar e-mails e anexos enviados com dados pessoais; adotar ferramenta de alarmística para visibilidade imediata de criação por utilizadores de regras de encaminhamento automático para contas externas; implementar ferramentas *antiphishing* e *antispam* para bloquear ligações e anexos com código malicioso; adotar controlos de segurança que permitam classificar e proteger as mensagens de correio eletrónico sensíveis; realizar ações de formação no sentido de capacitar os trabalhadores a operar os mecanismos de envio de mensagens de correio eletrónico.

d) **Proteção contra *malware*** — utilizar encriptação segura; criar sistema *backup* para cópias de segurança, separado das bases de dados principais e sem acessibilidade externa; reforçar o sistema com ferramentas *antimalware* com capacidade de verificar, detetar e bloquear, em tempo real, ameaças, incluindo do tipo *ransomware*.

e) **Utilização de equipamentos em ambiente externo** — definir regras para utilização de equi-

pamentos; armazenar dados em sistemas internos; permitir acessos apenas por VPN; bloquear as contas após várias tentativas inválidas de *login*; ativar a autenticação multifator; aplicar cifragem dos dados no sistema operativo; ativar *remote wi*pe e *find my device*.

f) **Armazenamento de documentos em papel que contenham dados pessoais** — utilizar papel e impressão durável; conservar documentação em local fechado, com controlo de humidade e temperatura, resistente ao fogo e inundação; controlar os acessos, com registo das respetivas data e hora, de quem acede e dos documentos acedidos; destruir documentos através de equipamento específico que garanta a destruição segura.

g) **Transporte de informação que integre dados pessoais** — adotar medidas para impedir a leitura, cópia, alteração e eliminação não autorizada de informação com dados pessoais; utilizar encriptação segura no transporte, em dispositivos de massa ou arquivo potencialmente permanente, como, por exemplo, *CD*, *DVD*, *PEN USB*.

> Notificação de violação de dados pessoais

A **violação da segurança** que provoque, ilícita ou acidentalmente, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a **dados pessoais** transmitidos, conservados ou sujeitos a qualquer tipo de tratamento, deve, em regra, ser notificada à CNPD, sempre que possível, no prazo máximo de 72 horas, quando seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

Mesmo que não seja exigível a **notificação à CNPD**, o responsável pelo tratamento está obrigado a **documentar** quaisquer violações de dados, nos termos do RGPD.

O responsável pelo tratamento está ainda obrigado a **informar os titulares dos dados** da ocorrência do evento de violação de dados, nos termos legalmente aplicáveis, quando for suscetível de implicar elevado risco para os direitos e liberdades das pessoas. O principal objetivo da notificação é prestar informações específicas acerca das medidas que devem tomar para se protegerem das consequências negativas da violação dos seus dados pessoais.

Consequentemente, o responsável pelo tratamento deve adotar **política interna para detetar e gerir incidentes de segurança** com impacto na proteção de dados pessoais e, quando o tratamento de dados for realizado por subcontratantes, ter **mecanismos de controlo eficazes** quanto à atuação dos subcontratantes

Artigo redigido de acordo com a legislação vigente em 13 de março de 2023.