PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

RGPD e a Segurança das Redes e Sistemas de Informação

Manual de Boas Práticas

Parte I

Deveres e responsabilidades das organizações

V1.0 16ABR18

Nota da Direção

No próximo dia 25 de maio entrará em vigor o novo Regulamento Geral de Proteção de Dados (RGPD), aplicável a todas as organizações, recaindo sobre estas a responsabilidade de o interpretar e fazer cumprir. Trata-se de um normativo que se baseia na autorregulação, cabendo por isso aos destinatários garantir a todo o tempo que se encontram em conformidade com as respetivas regras, sob pena de penalizações que todos pretendem evitar.

Para auxiliar quem, como nós, se encontra perante este desafio, o Gabinete Nacional de Segurança reuniu um conjunto de conceitos, informações e metodologias, com base nas melhores práticas adotadas na União Europeia e NATO relativas à segurança da informação, as quais, numa lógica transversal, foram vertidas num "Manual de Boas Práticas". Uma vez que a segurança dos dados pessoais inclui, mas não se limita, à implementação de medidas tecnológicas, este Manual deve ser entendido como um complemento aos requisitos técnicos mínimos que visam garantir uma arquitetura de segurança das redes e sistemas de informação que constam da Resolução de Conselho de Ministros nº. 41/2018.

Para maior facilidade de consulta, este Manual divide-se em três partes:

Parte I – Deveres e responsabilidades das organizações

Parte II – Contributos para políticas e procedimentos

Parte III – Segurança física

De realçar, no entanto, que este conjunto de documentos não deve ser considerado um normativo de aplicação obrigatória, nem mesmo um guia com carácter doutrinário, mas sim um algo que visa apenas partilhar as boas práticas que se julga adequado cada um utilizar, de acordo com a avaliação de risco que fizer da sua própria realidade e do estado de maturidade da sua organização no que respeita à salvaguarda da informação sensível, na qual se podem incluir os dados pessoais.

O Diretor-geral

António José Gameiro Marques

Assinado de forma digital por António José Gameiro Marques
Dados: 2018.04.18 18:30:25 +01'00'

António Gameiro Marques

CAlm

Índice

1. Proteção dos dados pessoais e das redes e sistemas de informação

Decorrente do Regulamento Geral sobre a Proteção de Dados (RGPD), uma organização, na qualidade de pessoa coletiva, autoridade pública, agência ou outro organismo, que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais, consubstancia-se, juridicamente, como entidade responsável pelo tratamento.

O RGPD vem, assim, exigir uma atenção cuidada às organizações que lidam com dados pessoais, obrigando à implementação de práticas e salvaguardas suplementares, bem como a repensar a forma como se encara a segurança da informação e das redes e sistemas de informação, cabendo ao responsável pelo tratamento o ónus de adotar medidas técnicas e organizacionais que garantam:

a) A salvaguarda das propriedades da informação, designadamente, a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio;

b) A segurança do tratamento, de modo a prevenir-se contra acessos não autorizados, divulgação não autorizada, modificação, remoção ou eliminação dos dados pessoais.

Consequentemente, o responsável pelo tratamento é o responsável por todos os aspetos da segurança (segurança física, lógica e operacional) das redes e sistemas de informação, sendo seu dever e responsabilidade:

- Criar e manter atualizado um registo de todos os ativos informacionais relativos a dados pessoais;
- Classificar os dados de acordo com critérios de sensibilidade e criticidade pré-definidos;
- Criar e manter atualizado um registo de todos os ativos tecnológicos (*hardware*, *firmware* e *software*);
- Garantir um nível de segurança forte dos dados pessoais e dos recursos de tratamento, dando prioridade aos mais sensíveis;
- Notificar eventuais violações de dados pessoais às autoridades de controlo;
- Designar de forma clara o encarregado da proteção de dados;
- Dar formação adequada a todos os utilizadores sobre segurança do sistema e dos dados pessoais.

É igualmente dever e responsabilidade do responsável pelo tratamento:

- Implementar diferentes tipos de mecanismos de segurança, criando diferentes camadas de proteção;
- Assegurar que cada mecanismo de segurança implementado contribui, separadamente e/ou em combinação com outros mecanismos, para atingir os objetivos de segurança;
- Anular ou, pelo menos, mitigar quaisquer deficiências na segurança que possam existir, mantendo o risco residual num nível aceitável;

- Garantir a segregação dos dados através da utilização de mecanismos físicos e lógicos apropriados para separar dados de diferentes tratamentos, criando repositórios distintos e com perfis de acesso diferenciados;
- Garantir a minimização dos dados, significando que serão tratados unicamente os dados absolutamente necessários para atingir a finalidade pretendida, pelo que os dados não necessários deverão ser descartados, preferencialmente com recurso a mecanismos automáticos;
- Adotar, sempre que necessário, medidas técnicas como a pseudonimização e a cifragem na proteção dos dados pessoais;
- Executar periodicamente o *software* de segurança e, com base nos resultados, determinar as mudanças na segurança que devem ser efetuadas;
- Efetuar alterações de *hardware*, *firmware* e *software* sem enfraquecer a segurança do sistema;
- Definir políticas e procedimentos relativos à gestão do ciclo de vida dos utilizadores, incluindo a criação, atribuição, manutenção e atualização das contas de utilizadores do sistema;
- Definir e manter atualizados os procedimentos e políticas de segurança que visem a operação segura do sistema e garantir a sua divulgação por todos os utilizadores;
- Sensibilizar todos os utilizadores para as respetivas responsabilidades individuais na segurança do sistema e dos dados pessoais;
- Obter a aceitação de todos os utilizadores, que tenham perfis com privilégios de escrita, leitura e eliminação de dados pessoais, das condições definidas num termo de responsabilidade (poderá ser em formato eletrónico);
- Garantir a assistência técnica a todos os utilizadores quando e onde necessário;
- Criar e manter registos (*logs*), de modo a permitir o rastreamento das atividades com impacto na segurança dos dados pessoais;
- Garantir a salvaguarda e a capacidade de recuperação de informações relevantes para a reposição total do sistema, incluindo os dados pessoais (*backups*);
- Assegurar a manutenção do sistema sem violar a sua segurança;
- Conduzir visitas técnicas para determinar se as medidas de segurança no local são suficientes e adequadas;
- Realizar auditorias internas e a entidades subcontratadas, cujos resultados devem ficar versados em relatório;
- Procurar a melhoria continua da segurança do sistema, através do planeamento e implementação de novas medidas, monitorização e verificação da adequação das mesmas e adoção de medidas corretivas sempre que necessário;

- Notificar qualquer incidente ou falha de *hardware* e/ou *software* com implicações na segurança dos dados pessoais, à entidade responsável pelo ciclo de vida do sistema;
- Determinar investigações nos casos de violações de segurança ou de suspeitas de violação;
- Definir de áreas de acesso restrito e controlado, sempre que considerado necessário, através:
  - De mecanismos que permitam o acesso às áreas seguras unicamente a pessoas autorizadas ("o que eu tenho", "o que eu sei" e/ou "o que eu sou");
  - Da criação e atualização de lista de pessoas autorizadas a aceder àquelas áreas;
  - Da criação e preservação de registos de acesso às áreas referidas.

2. Respeito pelos direitos do titular dos dados.

O responsável pelo tratamento deve ser capaz de respeitar os direitos do titular dos dados, designadamente:

- Direito de informação;
- Direito de acesso aos respetivos dados pessoais;
- Direito de retificação de dados inexatos;
- Direito ao apagamento (“direito a ser esquecido");
- Direito à limitação do tratamento;
- Direito de portabilidade de dados;
- Direito de oposição.

No domínio do exercício dos direitos, o responsável pelo tratamento deve garantir:

- A autenticidade da identificação do titular para o exercício dos seus direitos, não divulgando dados pessoais a terceiros não autorizados;
- A existência de documentação de todos os procedimentos de tramitação dos pedidos e registo em *logs* das operações que forem realizadas no sistema na sequência de pedidos de acesso, retificação, eliminação, ou limitação;
- O desenvolvimento de políticas organizativas e técnicas que permitam uma transmissão segura dos dados pessoais, de modo a que quando houver portabilidade dos dados (principalmente entre dois responsáveis pelo tratamento, mas também através do titular) estes sejam transmitidos em segurança e não sejam acedidos por terceiros não autorizados.

3. Estratégia para a segurança do tratamento de dados pessoais

O responsável pelo tratamento deve ter conhecimento, a todo o tempo, dos ativos de informação relativos a dados pessoais à sua responsabilidade, de modo a permitir a identificação inequívoca do estado da informação em todo o seu ciclo de vida e a garantir a sua segurança.

O responsável pelo tratamento deve, por conseguinte, definir políticas que garantam a segurança dos dados pessoais, em alinhamento com a estratégia superiormente definida para a segurança do tratamento de dados pessoais.

A estratégia para a segurança do tratamento de dados pessoais deve abranger:

- A criação;
- A classificação
- A priorização;
- A modificação;
- A transmissão;
- A recolha (independentemente do respetivo meio ou processo);
- A destruição;
- O armazenamento (incluindo a conservação);
- A pesquisa de dados.

4. Classificação, priorização e monitorização dos dados

De modo a assegurar uma proteção adequada dos dados pessoais, o responsável pelo tratamento deve incluir nas políticas de segurança procedimentos para a respetiva classificação, priorização e monitorização. Recomenda-se, no mínimo, que:

- Os dados pessoais sejam classificados de acordo com os critérios de sensibilidade e criticidade pré-definidos;
- Seja estabelecida uma priorização para a proteção dos dados pessoais, dando-se prioridade aos considerados mais críticos;
- Sejam efetuados e mantidos seguros os registos de atividades dos utilizadores (*logs*);
- Os serviços de apoio ao utilizador do sistema estejam preparados para responder a questões relacionadas com a segurança dos dados pessoais;
- Sejam realizadas verificações e avaliações periódicas a todo o conjunto de mecanismos de controlo e procedimentos de segurança implementados;
- Seja assegurada a monitorização das redes e sistemas de informação associados, podendo esta ser entregue a uma terceira entidade tecnicamente competente para o efeito.

5. Potenciais ameaças

O responsável pelo tratamento deve estar consciente das ameaças aos seus ativos informacionais e tecnológicos. Entende-se por ameaça qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a confidencialidade, integridade e/ou disponibilidade da informação ou sistemas de informação. Consoante a sua natureza, as ameaças podem ser de dois tipos:

a) Acidentais:

- Forças da natureza (i.e., inundações, tempestades, terramotos, etc.)
- Falhas da tecnologia por exemplo (i.e., *hardware*, *software*, energia, etc.)
- Fator humano (erros ou omissões)

b) Intencionais ou deliberadas:

- Espionagem
- Crimes (i.e., roubo, fraude, etc.)
- Intrusões
- Interceções
- Vandalismo
- Terrorismo
- Funcionários insatisfeitos e desonestos (*insiders*)
- Outros.

6. Vulnerabilidades dos ativos informacionais e tecnológicos

O responsável pelo tratamento deve conhecer as vulnerabilidades dos seus ativos informacionais e tecnológicos para protegê-los dos perigos mais comuns: destruição da informação, modificação ou alteração ilegítima da informação, roubo, remoção, eliminação ou perda da informação, divulgação não autorizada e interrupção ou negação de acesso aos dados.

Todos os utilizadores devem ser aconselhados a tomar precauções para evitar eventuais violações de segurança, entre as quais:

- O uso indevido do computador, que inclui, mas não está limitado a, violação da privacidade de outro utilizador, destruição deliberada de dados ou equipamentos, exploração de vulnerabilidades do sistema ou uso dos equipamentos informáticos da organização para fins pessoais;
- A violação de segurança, a qual abrange a divulgação de credenciais de acesso e autenticação, o contornar dos recursos de segurança do sistema, o acesso não autorizado, o ignorar o princípio da "necessidade de conhecer" e o desrespeito pelas regras de operação em segurança do sistema;
- O reporte imediato ao encarregado da proteção de dados, de forma expedita e devidamente aprovada, de qualquer violação da segurança do sistema, incluindo pessoal, *hardware*, *software*, comunicações, documentos ou segurança física.

A descoberta de novas vulnerabilidades deve ser prontamente comunicada ao responsável pela segurança do sistema.

7. Segurança e privacidade "*by design*" e "*by default*"

Nos casos em que os recursos de tratamento, designadamente as redes e sistemas de informação, são desenvolvidos internamente, o responsável pelo tratamento deve criar e reforçar a segurança e privacidade ao longo de todo o ciclo de vida do sistema, desde a fase de conceção (segurança e privacidade "*by design*").

O responsável pelo tratamento deve, ainda, optar por controlos de privacidade fortes, simples de implementar, difíceis de contornar e totalmente incorporados nas funcionalidades básicas do sistema (segurança e privacidade "*by default*").

Quando os recursos de tratamento são adquiridos a outra entidade, o responsável pelo tratamento deve impor requisitos de segurança e privacidade "*by design*" e "*by default*" e, sempre que possível, eleger equipamentos e/ou sistemas produzidos dentro da União Europeia.

8. Gestão do Risco

O responsável pelo tratamento deve avaliar previamente os riscos de segurança associados aos tratamentos de dados que realiza em concreto, quer quanto à natureza dos dados tratados (sensíveis ou carecendo de especial proteção) e universo de pessoas afetadas, quer quanto ao ambiente em que são tratados (em ambiente fechado, em redes e plataformas de comunicação partilhadas com transmissão de dados pessoais, em rede aberta, através de *websites*, etc…).

As medidas de segurança terão sempre de ser ajustadas à realidade de cada organização, pelo que a entidade responsável pelo tratamento deve assegurar que existe uma política clara de gestão do risco, focada na avaliação do risco e respetivo tratamento, para apoiar as escolhas efetuadas no âmbito da segurança da informação.

8.1 Avaliação do risco

Devem ser efetuadas avaliações do risco periodicamente, ou quando se verifiquem alterações significativas ou, ainda, quando são propostas. A avaliação de risco compreende:

a) A definição dos critérios de risco de segurança da informação – critérios de aceitação do risco e critérios de avaliação do risco - tendo em atenção que os indicadores devem ser mensuráveis e comparáveis;

b) A identificação dos riscos para a confidencialidade, integridade e disponibilidade da informação, bem como os responsáveis pelo risco;

c) A análise de risco, considerando a probabilidade relativa de ocorrência de cada risco identificado, conjuntamente como o seu impacto na segurança da informação caso se materializasse, de forma a determinar os níveis de risco;

d) A avaliação do risco comparando os resultados obtidos com os critérios de risco, de modo a estabelecer prioridades para o tratamento do risco.

8.2 Tratamento do risco

Tendo em conta os resultados obtidos na avaliação de risco, devem ser selecionadas as opções de tratamento de risco mais adequadas para cada caso, as quais passam pela eliminação, redução, transferência ou partilha do risco.

O tratamento do risco obriga à implementação de medidas de segurança de origem tecnológica, física e/ou procedimentais.

Embora seja impossível eliminar todos os riscos, devem-se implementar as medidas necessárias à obtenção de um risco residual aceitável.

Deve ser elaborado um plano de tratamento do risco onde seja explicitado inequivocamente as ações de resposta ao risco, os recursos necessários, os responsáveis, o prazo para a sua implementação, resultados esperados e a próxima avaliação dos resultados.

8.3 Melhoria continua

A gestão do risco deve ser um processo de melhoria contínua, sendo tão importante identificar os riscos como as oportunidades de melhoria, bem como a adequabilidade e eficácia das medidas implementadas de reposta ao risco. Como tal, é importante:

- Assegurar que as medidas de segurança são efetivamente implementadas;
- Monitorizar e avaliar a eficiência das medidas implementadas;
- Implementar medidas corretivas onde e sempre que necessário.

9. Auditorias

O responsável pelo tratamento é responsável pela condução de auditorias à segurança da informação e das redes e sistemas de informação, segundo requisitos previamente definidos para o efeito:

- Devem ser realizadas auditorias internas, periódicas e não programadas, para detetar não-conformidades, assim como, ações (potenciais e efetivas) que possam ter violado a segurança;
- No mínimo, devem ser recolhidos e registados os seguintes eventos auditáveis:
  - Registos dos equipamentos, serviços e aplicações que processem, transmitam ou armazenem dados pessoais;
  - Informações recolhidas dos sistemas de deteção e prevenção de intrusão;
  - Dados dos ativos de rede relevantes para os processos associados ao processamento, transmissão e armazenamento de dados pessoais.

Os resultados das auditorias devem ser mantidos por um período mínimo de 5 anos, sem prejuízo do definido pelas entidades competentes.

Todas as violações dos regulamentos de segurança, quebras dos controlos de segurança e incumprimento dos procedimentos de segurança, quer sejam identificados por meio da análise dos registos ou por outros meios, devem ser reportados às autoridades competentes de acordo com a legislação em vigor.

Devem também ser realizadas auditorias às entidades subcontratadas, de forma a detetar evidências de eventuais quebras de segurança.

10. Transferências de dados

O responsável pelo tratamento deve salvaguardar o princípio da legalidade e transparência nas transferências de dados.

Devem ser tomados cuidados especiais nas transferências de dados - em particular nos casos das transferências internacionais para países que, reconhecidamente, possuem uma legislação deficitária sobre a proteção de dados –, devendo as transferências ser efetuadas com base numa decisão de adequação, sujeitas a garantias, com respeito pelas regras vinculativas aplicáveis às empresas e demais cuidados constantes no Capitulo V do RGPD.

11. Investigação e notificação de incidentes

11.1 Investigação de incidentes

Dependendo das circunstâncias associadas à quebra de segurança, deve ser nomeada uma equipa de investigação para determinar:

- Se os dados foram ou não comprometidos;
- Em caso afirmativo, identificar a(s) pessoa(s) não autorizada(s) que tiveram ou tentaram ter acesso aos dados;
- Avaliar o impacto e o alcance da quebra de segurança:
  - No sistema dos dados pessoais e na entidade responsável pelo tratamento;
  - Nos direitos do respetivo titular;
- Avaliar e propor as ações adequadas (corretivas ou outras previstas na lei).

11.2 Notificação de incidentes

O responsável pelo tratamento deve garantir a implementação de um processo de notificação para os casos de quebra de segurança e/ou violação de dados, assim como, criar processos de gestão de incidentes e capacidades de deteção e resposta de acordo com a legislação nacional e da União Europeia em vigor.

Os processos de notificação devem permitir que a ação corretiva adequada seja aplicada em tempo útil, que o incidente seja reportado às entidades competentes e que a notificação ocorra no prazo máximo de 72 horas.

Devem ser notificadas todas as violações de dados, mesmo quando existam medidas de proteção como a cifragem ou a probabilidade do impacto daquele comprometimento ser baixo.

Os incidentes de segurança incluem:

- Ataques de códigos maliciosos (por exemplo, vírus, *trojan*, *worms* ou *scripts* não autorizados);
- Acessos não autorizados ou intrusões ao sistema;
- Utilização não autorizada de serviços ou equipamentos do sistema;
- Uso indevido do sistema (por exemplo, a utilização para fins diferentes àqueles a que o mesmo se destina);
- Recolha e divulgação não autorizada dos dados;
- Incidentes que envolvam o acesso privilegiado ao sistema;
- Incidentes com elementos de cifra;

- Incidentes com equipamentos periféricos e/ou de apoio;
- Incidentes com impacto significativo na organização;
- Negação e interrupção de serviços;
- Exfiltração, ou suspeita de exfiltração, de dados pessoais;
- Outros incidentes de causas naturais ou humanas (acidentais ou negligentes) que afetem o sistema.

A notificação deve conter, pelo menos, a seguinte informação:

- Descrição da natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
- Nome e contactos do encarregado da proteção de dados ou de outro ponto de contacto;
- Descrição das consequências prováveis da violação de dados pessoais;
- Descrição das medidas corretivas adotadas, inclusive, medidas para atenuar os eventuais efeitos negativos.

Deve ser criado e mantido um registo das notificações de incidentes de segurança, violações de segurança ou quebras de segurança verificadas.

Para fins de auditoria, o responsável pelo tratamento deve documentar todas as violações de dados pessoais, ou tentativas falhadas, contendo os factos relacionados com as mesmas, os respetivos efeitos e as medidas corretivas adotadas.

Recomenda-se um prazo mínimo de conservação da documentação acima referida de 5 anos.

Os planos de contingência devem incluir os processos de resposta imediata, de recuperação e o planeamento de implementação de medidas corretivas.

O encarregado da proteção de dados deve ter conhecimento de todos os procedimentos de notificação.

12. Sensibilização e formação

O responsável pelo tratamento deve garantir uma formação adequada na área da segurança da informação e das redes e sistemas de informação a todos os utilizadores, aos administradores do sistema e ao encarregado da proteção de dados:

- A formação dos utilizadores deve garantir a consciencialização para os comportamentos de segurança exigidos no âmbito da segurança da informação e da utilização segura dos sistemas de informação;
- As equipas de administração do sistema devem ser sujeitas a ações de formação que as capacitem para o correto desempenho das suas funções, no âmbito da proteção de dados pessoais;
- A função de encarregado de proteção de dados deve ser objeto de formação específica e especialmente adequada às suas responsabilidades.

No mínimo, todos os utilizadores devem ter consciência de que:

- A segurança das credenciais de acesso ao sistema e dados pessoais é também da responsabilidade do respetivo utilizador, que deve tomar as precauções necessárias para evitar e/ou negar o acesso dessas credenciais a terceiros;
- Devem ser tomadas precauções especiais ao executar os procedimentos de início de sessão (certificando-se, por exemplo, de que não há pessoas próximas que consigam visualizar os caracteres que estão a ser digitados);
- Não devem deixar a estação de trabalho sem vigilância quando a sessão está aberta;
- Nas situações em que é necessário deixar a estação de trabalho sem vigilância, devem ativar manualmente o bloqueio do ecrã;
- Devem proceder à alteração das credenciais de acesso sempre que essa alteração lhes for exigida ou que se suspeite do comprometimento das mesmas;
- No final do dia, devem encerrar a sua estação de trabalho.

As ações de formação e de sensibilização sobre a segurança da informação e utilização segura das redes e sistemas de informação devem ser obrigatórias para novos colaboradores e devem ser ministradas periodicamente a todos os colaboradores, pelo menos, uma vez por ano.