PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

RGPD e a Segurança das Redes e Sistemas de Informação

Manual de Boas Práticas

Parte III

Segurança Física

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 18:28:31 +01'00'

António Gameiro Marques

CAlm

V1.0 16ABR18

Índice

1. A segurança física 3
1.1 Em que consiste a segurança física 3
1.2 Para que serve a segurança física 3
1.3 Onde implementar a segurança física 3
2. Como escolher as medidas de segurança física a implementar 4
3. O princípio da "defesa em profundidade" 5
4. Como criar áreas seguras 6
4.1 Segurança das pessoas 6
4.2 Segurança das instalações 7
4.3 Segurança documental 8
4.4 Segurança eletrónica 9
5. Zonas técnicas seguras 10
6. Cuidados a ter na escolha, implementação e manutenção das medidas de segurança física 11
7. Segurança no transporte para fora das áreas seguras 12
8. Responsabilidades na segurança física 13

1. A segurança física

1.1 Em que consiste a segurança física

A segurança física é a aplicação de medidas físicas, técnicas e procedimentais de proteção para impedir o acesso não autorizado a informação considerada sensível, onde se inclui aquela que contém dados pessoais.

1.2 Para que serve a segurança física

As medidas de segurança física visam garantir que as ações sobre a informação sensível são, por um lado, efetuadas por pessoas autorizadas, responsáveis e que têm necessidade de conhecer e, por outro, são apoiadas por redes e sistemas de informação com o grau de disponibilidade, integridade, confidencialidade, autenticidade e não-repúdio necessários, sendo por isso importante:

a) Assegurar que os dados pessoais são manuseados e armazenados de forma adequada;

b) Negar ou dificultar a entrada fraudulenta ou forçada de pessoas não autorizadas;

a) Segregar o acesso aos dados pessoais com base na necessidade de conhecer;

b) Dissuadir, impedir e detetar ações não autorizadas;

c) Detetar e reagir rapidamente a eventuais quebras de segurança.

1.3 Onde implementar a segurança física

Devem ser implementadas medidas de segurança física em todas as instalações, edifícios, gabinetes, salas técnicas e em outras zonas onde sejam manuseados e/ou armazenados dados pessoais, incluindo áreas onde estão alojadas as redes e sistemas de informação que processam dados pessoais.

2. Como escolher as medidas de segurança física a implementar

A decisão sobre o grau de segurança física necessário deve ter em consideração os seguintes fatores:

a) O nível de criticidade da informação;

b) A quantidade e a forma (por exemplo, cópias em papel ou em suportes digitais) das informações tratadas e armazenadas;

c) O princípio da necessidade de conhecer;

d) A avaliação da ameaça local.

A combinação apropriada de medidas de segurança físicas a serem implementadas deve ser determinada com base no resultado da análise prévia do risco. A exigência das medidas deve ser proporcional ao risco identificado.

Para novas instalações, os requisitos de segurança física devem ser incluídos na sua conceção, desde a fase inicial do projeto e como parte integrante do planeamento. Para instalações existentes, os requisitos de segurança física devem ser implementados à medida do possível, respeitando as prioridades de segurança previamente estabelecidas.

3. O princípio da “defesa em profundidade”

Devem ser desenvolvidas medidas de segurança a diversos níveis, a fim de proporcionar o que se designa por "defesa em profundidade”:

- O primeiro nível deve definir a zona a ser protegida e impedir o acesso não autorizado à mesma;
- O segundo nível deve detetar o acesso não autorizado, ou as tentativas de acesso, e alertar o serviço de segurança ou as autoridades competentes;
- O terceiro e último nível deve conseguir retardar os intrusos durante o tempo suficiente para garantir a possibilidade de intervenção do serviço de segurança ou das autoridades competentes.

4. Como criar áreas seguras

Uma área segura obriga a que:

a) Seja estabelecido um perímetro visivelmente definido e protegido (barreira física);

b) Haja um controlo de todas as entradas e saídas de pessoas e, se aplicável, de veículos;

c) O acesso seja concedido apenas a pessoas devidamente habilitadas e especificamente autorizadas.

O controlo de entradas e saídas poderá ser visual (efetuado por agente de segurança ou rececionista), eletrónico, eletromecânico e/ou físico.

Dependendo da criticidade dos dados pessoais manuseados e armazenados, bem como do risco identificado, para serem criadas áreas seguras, devem ser observadas as medidas a seguir elencadas, parcialmente ou na totalidade, respeitando o princípio da proporcionalidade relativamente ao risco.

4.1 Segurança das pessoas

No que se refere à segurança das pessoas:

- As autorizações de acesso devem ser concedidas a pessoas especificamente autorizadas com base no princípio da necessidade de conhecer;
- Deve ser criada e mantida atualizada uma lista de pessoas autorizadas a aceder a cada uma das áreas seguras, a qual deve ser exposta em local bem visível junto da entrada;
- No caso de se optar por conceder acesso automático, a organização deve:
  - Ter capacidade para produzir e gerir os seus próprios códigos de acesso;
  - Definir procedimentos de gestão e de atribuição de códigos;
- Pessoas não autorizadas e que necessitem aceder às áreas seguras devem:
  - Solicitar previamente uma autorização específica e justificar esta necessidade;
  - Ser identificadas à entrada;
  - Ser sujeitas a uma verificação de segurança;
  - Ser acompanhadas durante toda a sua permanência nas referidas áreas;
  - Usar obrigatoriamente um passe identificativo de “Visitante”;
- Os serviços de limpeza e de manutenção (por exemplo, aos sistemas de climatização), quando efetuados por pessoas da organização sem autorização de acesso ou quando fornecido por empresa externa, devem ser supervisionados e as pessoas devem ser permanentemente acompanhadas enquanto permanecerem no interior das áreas seguras;
- Deve, ainda, ser criado um registo de entradas das pessoas que não constam da lista de acesso à área segura, o qual deve ser conservado durante um período mínimo de 12 meses.

4.2 Segurança das instalações

Quanto à segurança das instalações, as medidas incluem:

- Iluminação exterior ao longo de todo o perímetro;
- Sistema de vigilância (sistema de televisão em circuito fechado) com capacidade para cobrir continuamente todo o perímetro sem pontos mortos e, se possível, o interior das áreas seguras, ligado a uma central de monitorização com capacidade de gravação;
- Conservação das imagens por um período mínimo de 4 semanas;
- Implementação de um centro de segurança das instalações:
  - Guarnecido com pessoal, numa base de 24 horas, 7 dias por semana, devidamente instruído sobre o modo correto de proceder em caso de emergência;
  - Com capacidade para monitorizar todas as câmaras de vigilância e alarmes;
  - Equipado com um botão de emergência ligado às autoridades de segurança locais;
- O pessoal da segurança deve efetuar rondas periódicas e esporádicas, quer no interior quer no exterior das áreas seguras;
- As paredes, pisos e tetos devem ser de materiais que ofereçam a proteção e robustez necessárias (por exemplo, alvenaria, betão, tijolo ou material equivalente);
- As portas de acesso às áreas seguras devem ser construídas em madeira maciça, metal ou outro material que lhe confira solidez e resistência;
- A armação das portas de acesso deve oferecer a mesma resistência que a porta e os fiéis das dobradiças devem estar protegidos;
- As portas de acesso devem dispor de um sistema de controlo de acessos mecânico (por exemplo, chave, fechadura de segredo, tranca com cadeado), preferencialmente combinado com um sistema lógico (por exemplo, cartão de acesso com senha ou sistema de leitura biométrica);
- A porta de acesso deve dispor de um sistema de videoporteiro ou, no mínimo, de um olho-de-boi;
- No caso de as portas de acesso às áreas seguras disporem de chave:
  - Estas devem ser guardadas num chaveiro, devendo ser nomeado um fiel depositário;
  - Em alternativa, pode-se optar por um chaveiro eletrónico com códigos de acesso individuais;
- Devem ser elaboradas normas internas que estabeleçam os procedimentos para o controlo das chaves;
- No caso de as áreas seguras disporem de janelas, estas não devem permitir vistas para o interior (por exemplo, devem ser opacas ou equipadas com estores, cortinas ou outras proteções de efeito similar) e devem estar protegidas com grades que ofereçam resistência à intrusão física;
- No caso das áreas seguras disporem de varanda ou varandim, devem-se também utilizar portas de segurança;

- As áreas seguras devem estar providas de:
  - Sistema de alarme anti-intrusão ligado ao centro de segurança, caso exista;
  - Sistema de deteção de incêndios ligado ao centro de segurança, caso exista, e/ou à central de Bombeiros;
  - Sistema de extinção de incêndios;
  - Sistema de deteção de inundações ligado ao centro de segurança, caso exista;
  - Sistema de portas antipânico;
  - Destruidores de papel e de CD/DVD;
  - Sistema de energia elétrica alternativo (por exemplo, um gerador) para garantir os serviços vitais;
  - Saídas de emergência devidamente assinaladas;
- Devem ser definidos os procedimentos a seguir no caso de um alarme ser acionado.

4.3 Segurança documental

Para garantir a segurança documental:

- Deve ser efetuado e mantido atualizado o inventário dos dados pessoais sob o controlo da organização;
- Devem ser definidas políticas e procedimentos de revisão dos dados pessoais armazenados com vista à destruição dos que já não são necessários;
- No interior das áreas seguras devem existir cofres e armários apropriados (fechados com chave, fechadura de segredo ou tranca com cadeado), desejavelmente à prova de fogo, para guardar os dados pessoais mais críticos e as cópias de segurança (*backups*);
- As chaves dos cofres e armários não deverão ser levadas para fora do perímetro de segurança;
- As chaves e as combinações de segredo devem ser memorizadas pelas pessoas que precisam de as conhecer e devem ser guardadas em envelope duplo selado;
- Os envelopes que contêm as combinações de segredo devem também ser sujeitos a uma proteção adequada;
- As combinações de segredo deverão ser conhecidas pelo número mais restrito possível de pessoas;
- As combinações deverão ser modificadas:
  - Quando usadas pela primeira vez;
  - Sempre que haja uma mudança de pessoal;
  - Sempre que tenha ocorrido ou haja suspeita de ter ocorrido uma fuga de informação;
  - Quando sujeitos a manutenção;

- No mínimo, de seis em seis meses;

- Devem ser mantidos registos escritos das alterações das combinações de segredo;
- A reprodução dos documentos deve ser efetuada com recurso a máquinas fotocopiadoras fisicamente protegidas, apenas utilizadas por pessoas autorizadas (por exemplo, com acesso controlado por meio de código de acesso ou outro).

Embora os dados pessoais devam ser armazenados em armários fechados, adequados às áreas seguras, estes podem ser temporariamente armazenados fora das referidas áreas, desde que sejam adotadas medidas de segurança compensatórias, devidamente previstas nas políticas de segurança da organização.

4.4 Segurança eletrónica

Relativamente à segurança eletrónica:

- Servidores, sistemas de gestão de redes, controladores de rede e de comunicações, *routers*, *firewalls* - referentes a redes e sistemas de informação que tratam dados pessoais - devem ser acomodados em áreas seguras e, se possível, em bastidores com estruturas robustas, portas com fecho e proteções laterais/topo/base apenas removíveis com chave;
- Os terminais dos utilizadores devem estar, desejavelmente, localizados em áreas seguras, principalmente nos casos em que se tratem de dados pessoais críticos;
- Nas ligações entre equipamentos localizadas no interior da mesma área segura, bem como nas ligações entre diferentes áreas seguras dentro do mesmo edifício, deve utilizar-se, preferencialmente, fibra ótica;
- Não sendo possível a utilização de fibra ótica, recomenda-se uma separação mínima de 50 cm entre a cablagem das redes e sistemas de informação que processam dados pessoais e a restante cablagem (energia, telefones, dados, etc.);
- Dentro das áreas seguras apenas devem existir linhas de comunicação e dispositivos eletrónicos autorizados;
- Nas áreas seguras deve ser proibida a utilização de telemóveis, *smartphones* e de outros dispositivos eletrónicos com capacidade fotográfica:
  - Deve ser colocada à entrada da área segura a indicação da proibição dos dispositivos acima referidos;
  - Devem ser disponibilizados cacifos com chave à entrada das zonas seguras para guardar os dispositivos pessoais dos colaboradores e visitantes.

5. Zonas técnicas seguras

No caso de a informação ser considerada muito sensível e de forma a garantir que esta não é transmitida inadvertidamente ou ilicitamente para fora das zonas seguras, devem ser criadas zonas técnicas seguras, as quais requerem:

- A proteção contra escutas passivas não autorizadas (por exemplo, fuga de informações resultante de comunicações não seguras, escutas diretas ou emissões eletromagnéticas não intencionais) através da insonorização das paredes, portas, janelas, chãos e tetos das zonas seguras;
- A proteção contra escutas ativas não autorizadas (por exemplo, fuga de informações através de microfones, radio-microfones ou outros dispositivos implantados), devendo ser física e tecnicamente inspecionadas em intervalos regulares ou após qualquer entrada não autorizada ou suspeita dessa possibilidade.

Só deverá ser permitida a instalação de telefones em zonas tecnicamente seguras para uso interno e com uma proteção baseada em medidas de cifragem.

Devem existir registos escritos das aberturas dos cofres alojados nesta áreas contendo a identificação da pessoa, do dia e da hora.

Sempre que possível, os postos de controlo de acessos a estas áreas devem estar equipados com:

- Sistema de raio X para inspecionar o conteúdo dos volumes/bagagens que entram;
- Detetores de metal (pórtico e/ou portáteis).

6. Cuidados a ter na escolha, implementação e manutenção das medidas de segurança física

Ao adquirir-se equipamentos destinados ao reforço da segurança física (como cofres, máquinas de trituração, fechaduras de portas, sistemas de controlo de acesso eletrónicos, sistemas de alarme, entre outros), deve-se verificar se os mesmos satisfazem os requisitos exigidos ao fim a que se destinam.

A manutenção dos equipamentos/sistemas de segurança deve ser efetuada em intervalos regulares ou sempre que se considerar necessário, de forma a permitir a deteção atempada e a subsequente resolução de eventuais fragilidades ou deficiências. As ações de manutenção devem ter em conta o resultado das inspeções.

A eficácia das medidas de segurança, individuais e do sistema de segurança no geral, deve ser avaliada em cada inspeção.

7. Segurança no transporte para fora das áreas seguras

A transmissão de dados pessoais críticos para fora das áreas seguras, quer entre diferentes serviços dentro de um mesmo edifício quer entre diferentes instalações, deve ser efetuada através de redes e sistemas de informação protegidos por mecanismos de cifra. Quando tal não for possível, os dados pessoais devem ser transportados:

a) Em dispositivos eletrónicos de armazenamento (por exemplo, USB *Flash Drives*, *Hard Disks*, SSD) ou em papel se devidamente protegido (coberto ou embalado) de modo a impedir a observação e/ou a divulgação não autorizada do seu conteúdo;

b) No caso dos dados pessoais mais críticos, devem ser utilizados dispositivos eletrónicos de armazenamento com cifragem e autenticação.

Para além dos cuidados acima referidos, os dados pessoais devem estar permanentemente sob o controlo da pessoa que os transporta. Este cuidado assume particular relevância no transporte de dados pessoais críticos.

8. Responsabilidades na segurança física

Para se obter um grau satisfatório de segurança é necessário que todos conheçam as suas responsabilidades e saibam agir em conformidade. Para tal, devem ser elaboradas instruções claras, podendo ser produzidos procedimentos específicos para cada um dos diferentes grupos de utilizadores:

- Serviços de segurança;
- Utilizadores;
- Visitantes;
- Pessoal de manutenção e limpeza.

As instruções devem ser devidamente divulgadas e facilmente acessíveis por todos os colaboradores.