Manual de Boas Práticas

da

Freguesia de Barrancos

Introdução

O presente Manual de Boas Práticas visa divulgar e melhorar os conhecimentos sobre as regras relativas à proteção de dados pessoais, servindo como ponto de referência para os trabalhadores e membros do Executivo da Freguesia de Barrancos.

O guia é, deste modo, o primeiro documento em que o atual Executivo da Freguesia de Barrancos deixa patente o seu empenho em prestar aos seus membros um apoio real nas diversas áreas transversais, com o objetivo de contribuir para o melhoramento dos serviços prestados aos utentes.

Na linha desse objetivo, a disponibilização deste Manual de Boas Práticas ajudará a responder aos novos desafios suscitados pelo Regulamento Geral de Proteção de Dados.

Mais do que uma moldura legal, o RGPD introduz um conjunto de novas regras que são repercutidas no quotidiano das entidades e nas mentalidades dos seus agentes.

Também este não será, ao contrário da moda, um tema que deixará de estar na ordem do dia pouco tempo depois da sua entrada em funcionamento

Entre as novidades destacam-se a nomeação de um Encarregado de Proteção de Dados, as regras sobre a pseudonimização de dados, a alteração das regras sobre o consentimento, a implementação do direito ao esquecimento, a criação de obrigações acrescidas aos subcontratados, a introdução de coimas de valor elevado e obrigações relativas a quebras de segurança.

Este trabalho, na medida em que ajuda a sistematizar a leitura do RGPD, facilitando a sua interpretação e a compreensão holística, será de extrema importância para todos aqueles que, na Freguesia de Barrancos, se veem confrontados com esta nova realidade e que, face a ela, terão de tomar medidas em prol da conformidade, percebendo ao mesmo tempo os efeitos que aquelas terão no contexto da organização.

Este guia irá ajudar na sistematização dos processos internos da organização, no que concerne ao modo como recebe, trata, arquiva e posteriormente se desfaz, ou não, de dados pessoais.

Aliar este Manual de Boas Práticas às auditorias e avaliações periódicas ajudará a Freguesia de Barrancos a manter-se no rumo da conformidade (de forma autónoma).

Ao longo das próximas páginas os leitores terão acesso aos resumos de temas que constam do RGPD, na pretensão de ajudar a Freguesia de Barrancos a implementar novos procedimentos técnicos de tratamento de dados pessoais, assim como a adotar novos sistemas de gestão operacional de proteção de dados.

O Manual de Boas Práticas está dividido em capítulos tendo em vista a facilitação da sua leitura, principalmente por parte das pessoas que estão menos familiarizadas com esta temática.

Contudo, este é apenas o ponto de partida.

O conhecimento detalhado da regulamentação constante no RGPD permitirá compreender o que a Freguesia de Barrancos terá de fazer para respeitar este diploma legal.

Todavia, urge sublinhar que o RGPD não se resume a uma questão jurídica ou tecnológica.

Quando se passar para uma atitude prática face ao RGPD mais facilmente se fará uma abordagem sistemática ao problema.

Espera-se, assim, que este Manual seja útil, e que se transforme num verdadeiro guia prático.

Manual de Boas Práticas 7
Parte I 7
Deveres e responsabilidade das organizações 7
1.Proteção dos dados pessoais e das redes e sistemas de informação 8
2. Respeito pelos direitos do titular dos dados 10
3. Estratégia para a segurança do tratamento de dados pessoais 11
4. Classificação, priorização e monitorização dos dados 11
5. Potenciais ameaças 12
6. Vulnerabilidades dos ativos informacionais e tecnológicos 12
7. Segurança e privacidade “por concepção” e “por defeito” 13
8. Gestão do Risco 13
8.1 Avaliação do risco 14
8.2 Tratamento do risco 14
8.3 Melhoria contínua 15
9. Auditorias 15
10. Investigação e notificação de incidentes 15
10.1 Investigação de incidentes 15
10.2 Notificação de incidentes 16
11. Sensibilização e formação 16
Manual de Boas Práticas 18
Parte II 18
Contributos para políticas e procedimentos 18
1.Políticas e procedimentos operacionais 19
2.Acesso a dados pessoais dos júris em Procedimentos concursais 20
3.Pedidos de mobilidade / CV’s recebidos por e-mail 20
4. Realização de eventos 21
5. Proteção dos dados e dos recursos de tratamento 21
6. Gestão do Ciclo de Vida dos utilizadores 22
6.1 Criação de contas de utilizador 22
6.2 Definição de perfis de utilizador 23
6.3 Credenciais de autenticação (palavra-passe) 23
6.4 Bloqueio de contas dos utilizadores 24
6.5 Estações de trabalho 24
7. Registos de atividade 24

7.1 Registo e monitorização de atividade 24
7.2 Proteção dos registos de atividade 25
8. Cópias de segurança 25
9. Cifragem 25
10. Suportes de dados 26
10.1 Proteção dos suportes de dados 26
10.2 Eliminação dos suportes de dados 26
11. Manutenção 27
12. Subcontratação de serviços 28
13. Planos de emergência e de continuidade de negócio 28
Manual de Boas Práticas 30
Parte III 30
Segurança Física 30
1. A segurança física 31
1.1 Em que consiste a segurança física 31
1.2 Para que serve a segurança física 31
1.3 Onde implementar a segurança física 31
2. Como escolher as medidas de segurança física a implementar 31
3. O princípio da “defesa em profundidade” 32
4. Como criar áreas seguras 32
4.1 Segurança das pessoas 33
4.2 Segurança das instalações 33
4.3 Segurança documental 34
4.4 Segurança eletrónica 35
5. Implementação/manutenção de medidas de segurança física 36
6. Responsabilidades na segurança física 36
7. Glossário 38
Consentimento do Titular dos Dados 38
Dados Pessoais 38
Destinatário 38
Encarregado de Proteção de Dados ("DPO - Data Protection Officer") 38
Limitação do Tratamento 38
Minimização dos Dados 39
Oposição ao Profiling 39
Privacidade desde a conceção (“Privacy by Design”) 39

Privacidade por defeito (“Privacy by Default”) 39
Avaliação de Impacto 39
Pseudonimização 39
Responsável pelo Tratamento dos Dados Pessoais 40
Tratamento de Dados Pessoais 40
Terceiro 40
Violação de Dados Pessoais 40
Violação de Segurança (Incidentes de Segurança) 40

Manual de Boas Práticas

Parte I

Deveres e responsabilidade das organizações

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

2. Respeito pelos direitos do titular dos dados

3. Estratégia para a segurança do tratamento de dados pessoais

4. Classificação, priorização e monitorização dos dados

5. Potenciais ameaças

6. Vulnerabilidades dos ativos informacionais e tecnológicos

7. Segurança e privacidade “by design” e “by default”

8. Gestão do Risco

8.1 Avaliação do risco

8.2 Tratamento do risco

8.3 Melhoria continua

9. Auditorias

10. Transferências de dados

11. Investigação e notificação de incidentes

11.1 Investigação de incidentes

11.2 Notificação de incidentes

12. Sensibilização e formação

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

Decorrente do Regulamento Geral sobre a Proteção de Dados (RGPD), a Freguesia de Barrancos, na qualidade de pessoa coletiva, autoridade pública e organismo público, 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 à Freguesia de Barrancos, 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, a Freguesia de Barrancos 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;*
- *Nomear o encarregado da proteção de dados e publicitar a forma de o contactar;*
- *Dar formação adequada a todos os trabalhadores sobre segurança do sistema e dos dados pessoais.*

É igualmente dever e responsabilidade da Freguesia de Barrancos:

- *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 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

A Freguesia de Barrancos deve ser capaz de respeitar os direitos do titular dos dados, designadamente:

a) Direito de informação;
b) Direito de acesso aos respetivos dados pessoais;
c) Direito de retificação de dados inexatos;
d) Direito ao apagamento ("direito a ser esquecido");
e) Direito à limitação do tratamento;
f) Direito de portabilidade de dados;
g) Direito de oposição.

No domínio do exercício dos direitos, a Freguesia de Barrancos 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

A Freguesia de Barrancos 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.

A Freguesia de Barrancos 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, a Freguesia de Barrancos 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

A Freguesia de Barrancos 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

A Freguesia de Barrancos 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, à 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 "por concepção" e "por defeito"

Nos casos em que os recursos de tratamento, designadamente as redes e sistemas de informação, são desenvolvidos internamente, A Freguesia de Barrancos 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 "por concepção").

A Freguesia de Barrancos 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 "por concepção").

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

8. Gestão do Risco

A Freguesia de Barrancos 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 contínua

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 resposta 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

A Freguesia de Barrancos é responsável pela condução de auditorias à segurança da informação e das redes e sistemas de informação.

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.**

10. Investigação e notificação de incidentes

10.1 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).*

10.2 Notificação de incidentes

A Freguesia de Barrancos 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, a partir do momento do seu conhecimento.

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.*

11. Sensibilização e formação

A Freguesia de Barrancos deve garantir uma formação adequada na área da segurança da informação e das redes e sistemas de informação a todos os trabalhadores e aos membros do Executivo:

- *A formação dos trabalhadores e membros do Executivo deve garantir a consciencialização para os comportamentos de segurança exigidos no âmbito da segurança da informação e da utilização segura dos sistemas de informação;*
- *Os trabalhadores e membros do Executivo devem ser sujeitos a ações de formação que os capacitem para o correto desempenho das suas funções, no âmbito da proteção de dados pessoais;*

No mínimo, todos os trabalhadores e membros do Executivo 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.

Manual de Boas Práticas

Parte II

Contributos para políticas e procedimentos

1. Políticas e procedimentos operacionais

2. Proteção dos dados e dos recursos de tratamento

3. Gestão do Ciclo de Vida dos utilizadores

3.1 Criação de contas de utilizador

3.2 Definição de perfis de utilizador

3.3 Credenciais de autenticação (palavra-passe)

3.4 Bloqueio de contas dos utilizadores

3.5 Estações de trabalho

4. Registos de atividade

4.1 Registo e monitorização de atividade

4.2 Proteção dos registos de atividade

5. Controlo dos sistemas em produção

6. Instalação de novo hardware e software

7. Cópias de segurança

8. Cifragem

9. Computação em nuvem (Cloud)

10. Suportes de dados

10.1 Proteção dos suportes de dados

10.2 Eliminação dos suportes de dados

11. Instalação e proteção dos equipamentos

12. Manutenção

13. Subcontratação de serviços

14. Planos de emergência e de continuidade de negócio

1.Políticas e procedimentos operacionais

A operação segura e correta das redes e sistemas de informação obriga à definição de políticas e procedimentos operacionais:

- *As políticas de segurança devem ser escritas de forma clara, para que sejam facilmente compreendidas por todos os utilizadores do sistema;*
- *Todos os trabalhadores e membros do Executivo devem estar familiarizados com as políticas de segurança;*
- *As políticas de segurança devem estar disponíveis e acessíveis a todos os trabalhadores e membros do Executivo para rápida consulta;*
- *As políticas de segurança devem ser revistas periodicamente ou sempre que se justifique;*
- *Devem ser atribuídas responsabilidades coletivas e individuais, dentro da organização, no que concerne à segurança dos dados;*
- *Cada trabalhador e membro do Executivo deve ser individualmente responsável por respeitar as políticas e medidas de segurança implementadas;*
- *Todas as atividades realizadas no sistema devem estar sujeitas a monitorização e auditorias;*
- *Deve ser definida uma política rigorosa, indicando o grau de tolerância ou até mesmo a proibição absoluta, quanto:*
- *À utilização de dispositivos móveis;*
- *À utilização de dispositivos da organização fora das instalações da mesma, incluindo para fins pessoais;*
- *À utilização do correio eletrónico da organização;*
- *Ninguém deve ignorar os recursos de segurança do sistema, modificar qualquer programa ou aceder às áreas para as quais não tenham sido especificamente autorizados, ou tentar qualquer uma destas ações;*
- *O uso e o acesso não autorizados a equipamentos informáticos, programas e dados, e/ou a sua modificação, deve constituir uma infração de segurança que pode resultar em responsabilidade legal;*
- *A organização deve definir procedimentos internos, e quando aplicável ao nível da subcontratação, que visem lidar com os casos de violação de segurança dos dados pessoais;*

- *Os procedimentos internos acima referidos devem contemplar, no mínimo, medidas para deteção, identificação, investigação das circunstâncias, medidas mitigadoras, circuito da informação entre responsáveis e subcontratante, responsabilidades e, ainda, a notificação às autoridades competentes dentro dos prazos legais (72 horas), bem como a notificação aos titulares dos dados nos casos em que possa resultar num elevado risco para os próprios;*
- *Deve, ainda, ser definida uma política de gestão de risco para corroborar as decisões sobre as medidas mais ajustadas para eliminar ou, no mínimo, reduzir eventuais riscos.*

2.Acesso a dados pessoais dos júris em Procedimentos concursais

Para se obter um grau elevado de confidencialidade e de integridade dos dados pessoais dos titulares/candidatos, é necessário que os membros dos júris dos procedimentos concursais conheçam as suas responsabilidades e saibam agir em conformidade. Para o efeito, os membros que constituem estes júris devem conhecer a política de privacidade vigente na FREGUESIA DE BARRANCOS.

Ademais, a violação dos dados pessoais recolhidos no exercício daquelas funções pode implicar vários graus de responsabilidade (e.g. civil, disciplinar e penal), com o consequente pagamento de indemnização por danos materiais e imateriais.

3.Pedidos de mobilidade / CV's recebidos por e-mail

As questões laborais assumem um papel fundamental no âmbito do exercício das funções executivas/autárquicas.

Esta relevância não se prende com a gestão dos colaboradores e com os processamentos salariais.

Com efeito, urge estabelecer medidas de actuação padronizadas, de modo a garantir a confidencialidade e a integridade dos dados pessoais dos titulares/candidatos.

Assim, deverão ser criadas vias dedicadas através das quais os candidatos possam apresentar pedidos de mobilidade e candidaturas para procedimentos concursais de recrutamento.

Preconiza-se:

- A criação de uma conta de e-mail para candidaturas a procedimentos concursais de recrutamento;

Independentemente das opções assumidas, a política de privacidade deve ser facultada aos candidatos.

4. Realização de eventos

A realização de eventos (*e.g. desportivos, culturais, etc*) fazem parte do quotidiano das autarquias.

No âmbito da realização destes eventos torna-se necessário recolher dados pessoais.

Neste sentido, urge, não só, garantir a confidencialidade e a integridade dos dados pessoais dos intervenientes, mas também assegurar que os menores de idade obtêm o consentimento dos titulares das responsabilidades parentais.

Para o efeito, recomenda-se uma especial sensibilização dos trabalhadores da FREGUESIA DE BARRANCOS e dos membros do Executivo para esta temática.

Preconiza-se:

- A criação de minutas de consentimento (em formato papel/digital) adequadas à realidade acima descrita.

5. Proteção dos dados e dos recursos de tratamento

Para proteger os dados e os recursos de tratamento contra código malicioso (malware), devem ser implementados controlos de deteção e prevenção:

- *Deve ser instalado software antivírus e software anti-spam em todas as estações de trabalho e servidores que compõem a rede e sistema de informação;*
- *O software antivírus e o software anti-spam devem ser sempre devidamente licenciados e mantidos atualizados;*
- *A atualização do antivírus e do anti-spam deve ser, preferencialmente, automática;*
- *Deve-se verificar regularmente a presença de código malicioso em:*
- *Dados, sistema operativo instalado, pacotes de software e aplicações;*
- *Dispositivos de armazenamento removíveis;*
- *E-mails e anexos recebidos de fontes externas e internas;*
- *As portas USB que sejam necessárias devem ter políticas implementadas para impedir o acesso e abertura de ficheiros que possam executar programas potencialmente nocivos.*

Deve-se sensibilizar os *trabalhadores e membros do Executivo* para importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança, sempre que for detetado código malicioso.

Os trabalhadores e membros do Executivo também devem ter cuidados para evitar a introdução de código malicioso, pelo que devem adotar as seguintes ações preventivas:

- *Comunicar de imediato qualquer alerta apresentado pelo sistema antivírus;*
- *Evitar utilizar dispositivos de armazenamento removíveis;*
- *Se observar um comportamento suspeito do sistema, o utilizador deve parar imediatamente qualquer processamento em curso, desconectar o sistema potencialmente infetado da rede e notificar o responsável pela segurança.*

6. Gestão do Ciclo de Vida dos utilizadores

Devem existir políticas e procedimentos para atribuição de privilégios de acesso e utilização do sistema, de modo a garantir que o acesso aos recursos de tratamento dos dados pessoais é efetuado apenas por *trabalhadores e membros do Executivo* devidamente autorizados.

6.1 Criação de contas de utilizador

Devem ser estabelecidos procedimentos para a criação de contas dos trabalhadores e membros do Executivo (procedimento de registo):

- *O acesso ao sistema só pode ser concedido a quem tiver concluído, com sucesso, o procedimento de registo;*
- *Os pedidos de criação ou modificação de uma conta de utilizador, quando não exista um sistema de gestão de identidades e acesso (Identity and Access Management - IAM) devem ser efetuados através de formulários próprios, devidamente preenchidos e assinados;*
- *Devem existir igualmente regras específicas para contas de utilizadores genéricos (por exemplo, webservices);*
- *Quando a aprovação é concedida, deve ser gerada automaticamente uma nova conta individual para o utilizador e uma palavra-passe inicial (a qual deve também obedecer às regras definidas para as palavra-passe) que lhe irão permitir aceder às funções do sistema para as quais foi autorizado;*
- *Não devem ser permitidas contas compartilhadas.*

Deve ser criada e mantida atualizada uma lista de todas as pessoas autorizadas a usar o sistema e a extensão da respetiva autorização, isto é, a indicação dos respetivos privilégios de acesso.

Deverá ser disponibilizada ao encarregado da proteção dos dados a lista atualizada de utilizadores, para fins de controlo interno e verificação de conformidade.

6.2 Definição de perfis de utilizador

O acesso às funções do sistema deve ser refletido em privilégios de acesso (perfis) diferenciados, em razão da necessidade de conhecer e da segregação de funções, respeitando sempre o princípio do menor privilégio (isto é, cada utilizador deve possuir somente os privilégios necessários para realizar a sua função na organização).

Os perfis devem ser devidamente especificados e explicados aos *trabalhadores e membros do Executivo*.

6.3 Credenciais de autenticação (palavra-passe)

As credenciais de autenticação de cada *trabalhador e membro do Executivo* devem ser únicas e intransmissíveis.

No caso de autenticação ser efetuada por userID/palavra-passe:

- *No primeiro acesso ao sistema, deverá ser solicitado aos trabalhadores e membros do Executivo a alteração da palavra-passe inicial, cabendo-lhe a escolha da sua própria palavra-passe a qual deve ser única, fácil de lembrar (mas difícil de adivinhar), não repetida e apenas conhecida e memorizada pelo próprio;*
- *A palavra-passe deve ter no mínimo 9 caracteres e ser complexa, significando que a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a..z), letras maiúsculas (A..Z), números (0..9) e caracteres especiais (~! @ # $ % ^ & * () _ + | `- = \ {} []:"; '<>?,. /);*
- *Em alternativa, a palavra-passe poderá ser constituída por frases ou excertos de texto longo, sem caracter de "espaço";*
- *A palavra-passe deve ser alterada, no máximo, a cada 180 dias para perfis de utilizador e 90 dias para perfis de administradores de sistemas e bases de dados, ou quando for comprometida ou se suspeite que venha a ser comprometida;*
- *O sistema deve ser configurado para alertar os utilizadores de que devem alterar as respetivas palavras-passe, com uma antecedência adequada (máxima de 30 dias);*
- *A reutilização de palavras-passe anteriores deverá ser evitada, recomendando-se que não seja igual às últimas 4 palavras-passe.*

6.4 Bloqueio de contas dos utilizadores

As contas dos *trabalhadores e membros do Executivo* deverão ser automaticamente bloqueadas após 3 tentativas de autenticação mal sucedidas e bloqueadas manualmente se se suspeitar que a conta está a ser usada incorretamente.

O encarregado da proteção de dados deve ser alertado para as situações de bloqueio acima referidas através, por exemplo, de relatórios periódicos, de modo a poder detetar eventuais problemas ou desvios em relação à doutrina estabelecida.

As contas que deixam de ser necessárias devem ser bloqueadas, tornadas inativas ou eliminadas.

Devem ser definidas regras específicas para os casos de ausência prolongada de utilizadores (por exemplo, licenças, férias, baixas prolongadas, mudança de funções, entre outros), bem como procedimentos de reporte e de atualização destas situações.

6.5 Estações de trabalho

O bloqueio automático do ecrã da estação de trabalho deve ser ativado, preferencialmente, após 5 minutos de inatividade, podendo ser desbloqueado apenas com credenciais de acesso.

No final de cada ciclo de trabalho do utilizador, a respetiva sessão deve ser encerrada.

Deve ser previsto o encerramento automático da sessão de trabalho do utilizador em caso de inatividade por tempo superior a 3 horas, bem como o encerramento automático da estação de trabalho em caso de inatividade superior a 5 horas (excecionam-se necessidades de sessões ativas para efeitos de manutenção e administração de sistemas).

7. Registos de atividade

7.1 Registo e monitorização de atividade

Devem-se criar, atualizar e analisar periodicamente os registos de atividade (logs):

- *Os registos devem conter detalhes suficientes sobre as atividades dos trabalhadores e membros do Executivo que permitam a reconstrução do histórico de eventos (quem, onde, quando e ação efetuada sobre o dado pessoal);*

- *Os registos devem abranger qualquer atividade de criação, leitura, alteração, pesquisa, consulta, transmissão de dados a terceiros ou eliminação de dados pessoais, incluindo o registo temporal da ação e o respetivo resultado;*
- *Os registos de atividade devem ser* ***guardados por um período mínimo de 12 meses.***

7.2 Proteção dos registos de atividade

Devem-se estabelecer diretrizes para a proteção dos registos de atividade contra acessos não autorizados e modificações não autorizadas:

- *Devem-se definir políticas que visem a criação, manutenção, integridade, disponibilidade e segurança dos registos de atividade dos utilizadores;*
- *A gravação, os backups e a manutenção dos registos de atividade devem ser obrigatórios e incluir todos os tipos de eventos (eventos bem-sucedidos e falhados);*
- *Os acessos aos registos de atividade dos utilizadores devem ser limitados a pessoas devidamente autorizadas e para os fins legalmente previstos, nomeadamente auditorias.*

8. Cópias de segurança

Devem ser efetuadas cópias de segurança (backups) periódicas dos dados e do software para proteger contra perdas e danos, bem como para garantir, quando necessário, uma rápida e correta recuperação do sistema:

- *Deve ser definida uma política de salvaguarda da informação e do sistema que garanta a sua confidencialidade, integridade e disponibilidade e, ainda, a correta reposição dessa salvaguarda no sistema;*
- *Essa política deve, no mínimo, referir a periodicidade dos backups, a sua localização (a qual deverá ser diferente daquela onde se encontra o sistema em produtivo), o tipo (incremental, completo ou diferencial), o tempo de conservação, o acesso e a forma como devem ser armazenados.*

9. Cifragem

Nas situações em que é necessário recorrer aos mecanismos de cifragem, como por exemplo, na transmissão de dados pessoais sensíveis:

- *Devem ser tomadas todas as medidas necessárias para evitar que o material de cifra se torne acessível a pessoas não autorizadas;*
- *Devem ser definidos e implementados procedimentos de controlo para a segurança do sistema de cifra:*

- *Deve ser dada por escrito uma autorização específica ao pessoal autorizado a aceder ao material de cifra;*
- *Os procedimentos básicos para o uso de equipamentos de cifra devem estar detalhados nos respetivos manuais de operação;*
- *O pessoal com acesso ao equipamento de cifra deve estar familiarizado com os respetivos procedimentos de tratamento e manuseamento;*
- *Além disso, o pessoal deve ser proficiente na operação de equipamentos de cifra sob sua responsabilidade;*
- *Os trabalhadores e membros do Executivo fornecidos com equipamentos de cifra devem seguir as instruções de segurança emitidas especificamente para esse dispositivo;*
- *Deve existir um suporte mínimo à gestão do ciclo de vida de chaves de cifra preparado para as criar, revogar e substituir.*

10. Suportes de dados

10.1 Proteção dos suportes de dados

Os suportes de dados devem ser protegidos contra acessos não autorizados, utilização indevida ou violação da respetiva integridade:

- *A organização deve disponibilizar os seus próprios suportes de dados eletrónicos;*
- *Devem ser autorizados apenas os suportes de dados da organização, devendo ser proibida a utilização de suportes de dados pessoais;*
- *A utilização dos suportes de dados removíveis deve ser gerida em todas as suas fases, incluindo a aquisição, distribuição, utilização e destruição;*
- *Devem ser definidos procedimentos de destruição de emergência para serem executados em circunstâncias excecionais;*
- *Antes da eliminação ou reutilização de equipamentos que contenham suportes de dados, deve-se verificar se todos os dados foram efetivamente removidos ou eliminados;*
- *No caso dos suportes de dados em papel, a impressão e/ou cópias de documentos contendo dados pessoais devem ser limitadas ao estritamente necessário;*
- *Todos os utilizadores devem garantir que nenhuma impressão e/ou cópia fica esquecida na impressora/fotocopiadora.*

10.2 Eliminação dos suportes de dados

Os suportes de dados devem ser eliminados de forma segura, quando deixarem de ser necessários, através da utilização de procedimentos formais:

- *Devem ser definidos procedimentos formais para destruição dos suportes de dados, de forma a garantir que os dados são completamente eliminados;*
- *Devem ser eliminados todos os dados armazenados nos equipamentos em fim de vida;*
- *Os equipamentos em fim de vida devem ser desmagnetizados e/ou fisicamente destruídos;*
- *Os documentos em papel devem ser destruídos com recurso a máquinas trituradoras próprias;*
- *No caso de dados pessoais críticos, a destruição dos suportes de dados (eletrónicos e em papel) deve ser testemunhada presencialmente pelo encarregado da proteção de dados;*

Aquando da destruição de suportes de dados contendo dados pessoais críticos, devem ser elaborados certificados de destruição, de acordo com a Portaria n.º 412/2001.

11. Manutenção

Deverão existir cuidados acrescidos na manutenção dos equipamentos e/ou sistema, particularmente nos casos em que manutenção é assegurada por terceiros:

- *O processo de escolha da empresa subcontratada para o efeito deve incluir critérios de idoneidade;*
- *Salvo situações urgentes, as ações de manutenção devem ser programadas;*
- *As ações de manutenção devem ser realizadas preferencialmente nas instalações do responsável pelo tratamento e previamente autorizadas;*
- *As ações de manutenção que representem alta criticidade não deverão ser efetuadas por uma só pessoa;*
- *Deve ser exigido um registo escrito e detalhado de todas as ações de manutenção efetuadas;*
- *Devem ser eliminados todos os dados armazenados nos equipamentos antes de estes serem enviados para a manutenção;*
- *Quando existam, os discos rígidos dos equipamentos periféricos devem ser previamente removidos;*
- *O contrato de manutenção deve prever a penalização da empresa subcontratada nos casos de apropriação indevida, perda ou alteração dos dados.*
-

12. Subcontratação de serviços

Nos casos em que é necessário subcontratar serviços deve ser celebrado um contrato entre a entidade responsável pelo tratamento e a entidade subcontratada onde constem cláusulas contratuais com orientações explícitas quanto à segurança dos dados pessoais, designadamente:

- *Descrição exaustiva das responsabilidades e funções a desempenhar por cada uma das partes;*
- *Não permitir o acesso remoto aos sistemas, salvo casos excecionalmente urgentes e nunca sem uma autorização prévia devidamente documentada;*
- *As intervenções nas redes e sistemas de informação devem ser realizadas, preferencialmente, nas instalações do responsável por razões de segurança e controlo;*
- *As intervenções devem ser programadas e previamente autorizadas pela entidade responsável pelo tratamento;*
- *Deve existir um registo escrito com a descrição detalhada de todas as intervenções;*
- *Credenciação de segurança do pessoal sob o controlo das entidades subcontratadas, quando aplicável;*
- *Segregação dos ambientes de desenvolvimento e de produção através da atribuição de diferentes privilégios de acessos;*
- *A entidade subcontratada deve ser devidamente informada sobre as suas responsabilidades na proteção dos dados pessoais, devendo indicar formalmente, aquando da assinatura do contrato, que compreende e aceita as suas responsabilidades neste o domínio.*

13. Planos de emergência e de continuidade de negócio

Deve ser elaborado um plano de emergência e de continuidade de negócio, que inclua o plano de contingência, backups e os procedimentos de recuperação em caso de desastre (plano de recuperação de desastre), bem como a atribuição de responsabilidades:

- *Estes planos destinam-se a todas as instalações disponíveis e incluem a manutenção de backups de dados, programas essenciais do sistema e a identificação de meios alternativos para manter a continuidade do negócio;*
- *As redundâncias existentes, bem como os meios utilizados na recuperação, devem possibilitar o mesmo nível de segurança dos dados que os sistemas produtivos;*
- *Nestes planos devem estar devidamente explicitados os procedimentos a seguir;*

- *Os procedimentos de evacuação em caso de sinistro devem acautelar a salvaguarda dos dados pessoais, incluindo os contidos nos equipamentos portáteis;*
- *No caso de uma evacuação de emergência, os equipamentos informáticos devem ser protegidos por bloqueio ou mesmo desligados, desde que tal ação não coloque ninguém em perigo;*
- *Os procedimentos de emergência devem ser do conhecimento de todos os colaboradores e testados, no mínimo, uma vez por ano;*
- *A ativação do plano de recuperação desastre deve ser entendida como uma medida interna provisória até o sistema recuperar a capacidade total, devendo ser respeitados os procedimentos nele estabelecidos.*

Manual de Boas Práticas

Parte III

Segurança Física

1. A segurança física 1.1 Em que consiste a segurança física

1.2 Para que serve a segurança física

1.3 Onde implementar a segurança física

2. Como escolher as medidas de segurança física a implementar

3. O princípio da “defesa em profundidade”

4. Como criar áreas seguras

4.1 Segurança das pessoas

4.2 Segurança das instalações

4.3 Segurança documental

4.4 Segurança eletrónica

5. Zonas técnicas seguras

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

7. Responsabilidades na segurança física

8. Acesso a dados pessoais dos júris em Procedimentos concursais

9. Pedidos de mobilidade / CV’s recebidos por e-mail

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 trabalhadores e membros do Executivo especificamente autorizadas com base no princípio da necessidade de conhecer;*
- *Deve ser criada e mantida atualizada uma lista de trabalhadores e membros do Executivo autorizados 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) ligado a uma central de monitorização;*
- *Equipado com um botão de emergência ligado às autoridades de segurança locais;*

- *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).*
- *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;*
    - *No caso das 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.*

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;*

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. Implementação/manutenção de 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.

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.

6. 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.

7. Glossário

Consentimento do Titular dos Dados

Qualquer manifestação de vontade, livre, específica, informada e explicita, nos termos da qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objecto de tratamento.

Dados Pessoais

Qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (”titular dos dados”); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um identificador como o nome, número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, económica, cultural ou social.

Destinatário

A pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro.

Encarregado de Proteção de Dados ("DPO - Data Protection Officer")

Pessoa designada pela organização que estará envolvida em todas as questões relacionadas com a proteção de dados pessoais.

Esta função deve ser atribuída sempre que o processamento for levado a cabo por uma entidade pública; se verifique a monitorização constante de indivíduos em larga escala; ou exista processamento de dados sensíveis em larga escala. As principais funções do encarregado de proteção de dados envolvem informar e aconselhar a empresa sobre a conformidade da proteção de dados; aconselhar sobre a avaliação do impacto da proteção de dados; monitorizar a conformidade da proteção de dados, que inclui, por exemplo, formar a equipa e realizar auditorias relacionadas com esta área; e cooperar e atuar como ponto de contacto com as autoridades de proteção de dados.

Limitação do Tratamento

Inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro.

Minimização dos Dados

Significa que os dados pessoais recolhidos devem ser limitados ao que é necessário relativamente às finalidades para as quais são tratados.

Oposição ao Profiling

Os titulares dos dados têm direito a opor-se ao uso de profiling, ou seja, qualquer forma automatizada de processamento de informação pessoal, com o objetivo de avaliar e tipificar indivíduos com base nos seus dados pessoais.

Privacidade desde a conceção ("Privacy by Design")

Significa levar o risco de privacidade em conta em todo o processo de conceção de um novo produto ou serviço, em vez de considerar as questões de privacidade apenas posteriormente. Tal significa avaliar cuidadosamente e implementar medidas e procedimentos técnicos e organizacionais adequados desde o início para garantir que o tratamento está em conformidade com o RGPD e protege os direitos dos titulares dos dados em causa.

Privacidade por defeito ("Privacy by Default")

Significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por defeito, apenas será recolhida, utilizada e conservada para cada tarefa, a quantidade necessária de dados pessoais. Esta obrigação aplica-se à extensão do seu tratamento, ao prazo de conservação e à sua acessibilidade. Estas medidas asseguram que os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Avaliação de Impacto

Permite que a organização encontre problemas nas fases iniciais de qualquer projeto, reduzindo os custos associados e danos à reputação que poderiam acompanhar uma violação das leis e regulamentos de proteção de dados.

Pseudonimização

Tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Responsável pelo Tratamento dos Dados Pessoais

A pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais.

Subcontratante

A pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Tratamento de Dados Pessoais

Qualquer operação ou conjunto de operações efetuados sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, bem como a limitação, apagamento ou destruição.

Terceiro

Pessoa singular ou coletiva, autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular de dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja autorizado a tratar os dados.

Violação de Dados Pessoais

Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Violação de Segurança (Incidentes de Segurança)

Evento com um efeito adverso real na segurança das redes e dos sistemas de informação, tal como um acesso não autorizado ao sistema de informação.