Your Company

Formulário interno nº _____ versão _____

Nota importante: Este documento é gratuito e de utilização livre. Pode ser alterado, tanto nos aspetos gráficos como no texto. Esta é a versão 1.0 e será atualizada mensalmente.

A única condição de utilização é manter uma referência, em rodapé, ao seu autor ou alternativamente fazer um like na página de facebook https://www.facebook.com/CiberSeguran%C3%A7a-1555249724772653/ .

Todo o texto com fundo amarelo e exemplos dados, deverão ser eliminado antes de produzir o documento final.

Solicite o Word Editável através do Email geral@ciberseguranca.org

Políticas de gestão, Proteção e Privacidade de Dados Pessoais

ao abrigo do novo

Regulamento Geral de Proteção de Dados Pessoais

Equipa:

Elaborado por:		Função:	Data:
Revisto por:		Função:	Data:
Aprovado por:		Função:	Data:

Data de Publicação: ___/_____/_____

Validade/ Próxima Revisão: ___/_____/_____

Contents

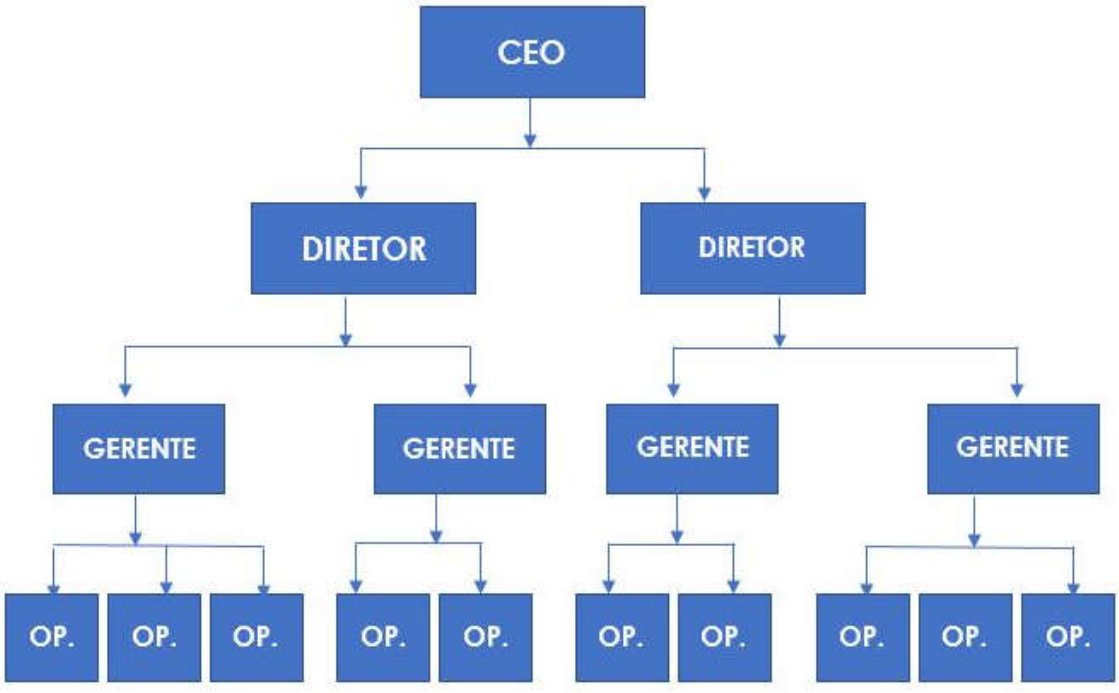
1. Enquadramento

Explicar resumidamente o Âmbito de atuação da empresa/organização, história, missão, políticas de qualidade, certificações (ex. ISO 9001 caso tenha).

a. Organização

Explicar resumidamente a organização da empresa preferencialmente anexando um organigrama, identificando claramente as direções e os serviços que tratam dados pessoais.

Exemplo:



Pode utilizar uma ferramenta online e de forma gratuita desenhar o seu organigrama:

https://www.smartdraw.com/organizational-chart/organogram-template-maker.htm

b. Recursos Humanos

Identificar e descrever o processo de recrutamento de recursos humanos, ou fazer referencias aos processos específicos de contratação, avaliação, formação, segurança no trabalho, etc. Todos os formulários (papel ou informáticos) que têm dados pessoais de colaboradores (sejam contratados, consultores ou trabalhadores eventuais) devem ser identificados neste ponto.

Exemplo:

Processo	Suporte/formulário	Tipo dados Pessoais	Observações
Candidaturas	Informático/Website	Dados demográficos Histórico profissional	Todos os dados são eliminados apos o processo de contratação terminar
Contratação	Papel/Impresso XXX	Dados demográficos Histórico profissional	Todos os dados são conservados por um período de X anos de acordo com a legislação laboral
Processamento Vencimentos	Informático/ Sistema XXX	Dados demográficos Dados Financeiros	Todos os dados são conservados por um período de X anos de acordo com a legislação laboral. Existe partilha de informação com TOC, para processamento de salários e subsídios.
Medicina no Trabalho	Procedimento QX Papel/Impresso XXX Especificar ou criar documento próprio	Dados demográficos Histórico profissional	Todos os dados são conservados por um período de X anos de acordo com a legislação laboral. Existe partilha de informação com empresa XYX, para consultas de medicina no trabalho e demais atividade médica de contexto laboral.
Acidentes de Trabalho	Papel/Impresso XXX	Dados demográficos Histórico profissional	Todos os dados são conservados por um período de X anos de acordo com a legislação laboral. Existe partilha de informação com as entidades oficiais, no âmbito do contexto laboral.
Etc.	Etc.	Etc.	
Festas de Natal	Papel/Impresso XXX	Dados do agregado familiar do colaborador.	No âmbito das festas de Natal, são solicitados os dados dos familiares, para ofertas que normalmente acontecem na altura do Natal..

c. Recursos Tecnológicos

Identificar e descrever todos os sistemas de informação (aplicações informáticas) sejam elas instaladas na empresa/organização ou na cloud.

Identificar todos os ficheiros Excel, word, powerpoint etc, que têm dados pessoais de colaboradores, fornecedores (informação individual das pessoas dos fornecedores), clientes e outras pessoas singulares que se relacionem com a empresa/organização.

Exemplo:

Sistema	Fornecedor	Tipo dados Pessoais	Observações
Office 365	Microsoft	Nomes e contactos pessoais de fornecedores, colaboradores e outras pessoais individuais com quem é trocada correspondência eletrónica. Outros dados que circulam por email (ex. dados demográficos de colaboradores em processos de RH, dados de clientes para efeitos de faturação, etc.)	É política da empresa, que o email institucional deve ser usado apenas para fins profissionais. Todos os colaboradores têm conhecimento dessa política, através do documento "Politicas de Utilização de Recursos da Empresa" e aceitam que caso haja cessação de funções, esse email passará a ser encaminhado para um email geral por um período nunca inferior a 6 meses (mesmo que o seu email tenha o seu nome no endereço). São usadas passwords fortes e ficheiros encriptados sempre que há necessidade de transmitir por email dados pessoais sensíveis. Existe ainda formação específica neste domínio (ver politicas de formação da empresa) .
ERP	XXX	Nomes e contactos pessoais de fornecedores de produtos e serviços	Para efeitos de suporte, garantia e suporte pós-venda podem ser registados dados pessoais (dos técnicos alocados a projetos específicos). Nesses casos, o titular dos dados pessoais dará o seu

			consentimento, através do template/formulário XXXX. Esses dados serão arquivados por um período de XXX anos.
CRM	XXX	Nomes e contactos pessoais de clientes	Para efeitos de faturação, garantia e suporte pós-venda e conservação legal, existirá a necessidade de conservar dados pessoais após a prestação do serviço. Nesses casos específicos, existe um consentimento dado pelo cliente, que aceita que os seus dados se mantenham arquivados na nossa organização pelo período de XXX anos. Ver o template relativo ao consentimento de clientes, para efeitos de suporte e manutenção pós-venda XXXXX.
RH	XXXX	Nomes e contactos pessoais de colaboradores. Histórico profissional Assiduidade Georreferenciação	Todos os dados pessoais armazenados para efeitos laborais, serão realizados ao abrigo da legislação laboral. Outros dados pessoais como georreferenciação poderão ser alvo de consentimentos específicos por parte do seu titular.
Acesso à Internet	Acesso direto através do Operador XXXXXX	Endereço IP, cookies de sessão, entre outros identificadores electrónicos que possam identificar uma pessoa individual.	É política da empresa, que a internet institucional deve ser usado apenas para fins profissionais. Todos os colaboradores têm conhecimento dessa política, através do documento "Politicas de Utilização de Recursos da Empresa" e aceitam que haja monitorização dos sites visitados e produção de relatórios com essa informação. Existe ainda formação específica neste domínio (ver politicas de formação da empresa) . Devem ser usadas sempre passwords fortes para registo em plataformas

			online e usar sempre formas seguras (ex. ficheiros encriptados, sites HTTPs, etc.) sempre que há necessidade de transmitir através da internet dados pessoais sensíveis.
Etc.	Etc.	Etc.	
Ficheiro EXCEL	Interno	Lista de todos os funcionários ativos da empresa e respetivos números de telefone pessoais	Servindo como plano de contingência, é mantida uma lista telefónica de todos os colaboradores da empresa. Esta lista tem os contactos pessoais para efeitos de contacto de emergência. Existe um consentimento dos colaboradores, e esta informação é apenas usada pela direção de recursos humanos ou pela administração em contexto de episódios de elevada urgência.

d. Clientes

Caracterizar, de forma muito resumida, o tipo de clientes ou entidades individuais a que a empresa /organização presta serviços (ou vende produtos). É muito importante que se identifiquem nesta fase todas as categorias de clientes.

Exemplo:

Tipo de Cliente	Grupo	Tipo dados Pessoais	Observações
Cliente sem serviços de garantia	Cliente pontual	Nome, NIF e contactos pessoais	
Cliente com serviços de garantia	Cliente Fidelizado	Nome, NIF, morada e contactos pessoais (telefone e email)	É necessário manter os os dados pessoais por um período nunca inferior ao período de garantia + 6 meses.
Cliente fora da União Europeia			RGPD não aplicável, embora sejam seguidos os mesmos princípios de privacidade e segurança de dados pessoais.

Etc.	Etc.	Etc.	**Existem especificidades de cada grupo de clientes que podem ser aqui indicados.**

e. Informação existente na organização

Sem prejuízo da existência de outras fontes de informação (com outras categorias de dados), são identificadas as seguintes localizações físicas e lógicas (para cada uma das alíneas anteriores **b)**, **c)** e **d)**

Exemplos:

Informação	Localização	Suporte	Backup e plano de contingência	Licitude para tratamento
Base De Dados de RH	Servidor de Recursos Humanos (RH-SERVER)	Base de Dados SQL Server	Backup diferencial diário para disco (localização serv-backups: D: Backup semanal completo para Tape armazenada no arquivo da empresa. **Responsabilidade: Técnico XXXXX**	Legislação Laboral; Consentimento dos colaboradores para os pontos x, y e Z Dados são conservados por XX anos Há partilha de informação especifica com TOC e Empresa de medicina no trabalho.
Base de Dados de Clientes	Servidor de CRM (Tiger-Server)	Base de Dados MySQL (ex. TigerCRM)	Backup diferencial diário para disco (localização serv-backups: D: Backup semanal completo para Tape armazenada no arquivo da empresa. **Responsabilidade: Técnico XXXXX**	Legislação aplicável a transações comerciais e direito do consumo; Consentimento dos colaboradores para os casos x, y e Z Dados são conservados por XX anos
Email Office 365	Cloud	Digital	Backup e plano de contingência assegurado pelo fornecedor de serviços **Contacto 24h/dia : XXXXXXXXX**	Consentimento e código de conduta.
Formulário YY	Dossier Colaborador	Papel	Não existe política de backup	Consentimento do Colaborador e Código de Conduta.
Contrato colaboradores	Dossier Colaboradores	Papel	Copia no arquivo secundário.	Consentimento do Colaborador e contrato de trabalho. Há partilha de informação com TOC e Empresa de medicina no trabalho.

Listagem YY	Servidor Partilhas (pasta RH)	Excel	Backup semanal.	Consentimento do Colaborador e Código de Conduta. Documento protegido e acesso limitado aos serviços de RH

2. Política de Privacidade

A política de privacidade é algo inerente a cada área de negócio e depende muitos dos canais utilizados para relacionamento com os clientes, fornecedores e colaboradores.

É possível ter várias politicas de privacidade, para cada área ou canal onde se gerem dados pessoais. Recomenda-se que sejam criadas pelo menos duas políticas de privacidade: Uma para canais online (websites) e outra para a área de gestão de recursos humanos. É também muito ntural que a política de privacidade para recursos humanos já exista sob a forma de código de conduta. Nestes casos, bastará complementar o código de conduta com elementos específicos relacionados com o RGPD (ex. precauções e preocupações no registo, tratamento, arquivo e partilha de dados pessoais.)

Dependendo da análise previa feita no capitulo 1, aconselha-se a:

a. Criar uma visão de programa comum a toda a organização
b. Tratar a mesma como imperativo comercial
c. Tornar os funcionários familiarizados com as políticas através de formação contínua, lembretes no email, avisos nas áreas comuns, etc
d. Deve ser alvo de uma avaliação contínua de risco
e. Em qualquer momento deve ser dada a possibilidade ao titular de dados de consultar os seus dados pessoais, solicitar a correção/retificação ou até mesmo que os dados sejam apagados (direito ao apagamento).
f. Os direitos de um determinado titular à portabilidade dos dados devem ser tratados tendo em conta eventuais direitos de terceiros, na medida em que alguma informação pode estar relacionada com esses terceiros.

Não deve incluir na sua política de privacidade:

a. Textos pre-formatados e genéricos.
b. Objetivos específicos ou métricas de processos ou aspectos dependentes de tecnologias
c. Situações em que atribui responsabilidade a uma única pessoa

Os programas de privacidade exigem atenção e monitorização ao longo do tempo e por isso deve prever mecanismos de auditoria e controlo. É pos isso importante incluir este aspecto na sua politica de qualidade e conformidade.

A adesão ao programa/política de privacidade deve ser monitorada, medida e aprimorada, continuando a demonstrar eficácia e benefício. Quando implementado corretamente, um programa de privacidade demonstra a responsabilidade. Também facilita o caminho para uma auditoria holística. Em algumas situações, certificar as operações de acordo com os padrões preferidos pode ajudar na instalação da confiança tanto dos reguladores quanto dos clientes.

Deve ser abandonada a ideia de "implementar e esquecer" e tratar a conformidade da privacidade e segurança dos dados pessoais como um projeto contínuo que deve ser mantido mesmo depois da data de 25 de maio de 2018, como é o caso do Regulamento Geral de Proteção de Dados da UE (GDPR).

a. Exemplos de políticas de privacidade para colaboradores:

O código de Conduta da empresa XXX pretende constituir uma referência para os seus clientes, no que respeita aos padrões de conduta, quer no relacionamento entre colaboradores, quer no relacionamento com clientes e fornecedores, contribuindo para que a empresa XXX seja reconhecida como um exemplo de excelência, integridade, responsabilidade e rigor.

A empresa XXX tem implementado continuamente uma política de valorização e capacitação do seu ativo mais significativo - os recursos humanos. Implementámos processos contínuos de qualificação com o objetivo de adquirir e manter as melhores competências profissionais, ajustando as mesmas de forma dinâmica aos meios económicos e financeiros da organização e das especificidades do mercado de trabalho.

O presente Código de Conduta aplica-se a todos os colaboradores da empresa, entendendo-se como tal todas as pessoas que prestem atividade na mesma, incluindo os membros dos corpos sociais e demais dirigentes, quadros, trabalhadores e colaboradores. Este código de Conduta não dispensa nem substitui outras regras de conduta ou deontológicas, de fonte legal ou de qualquer outra natureza, aplicáveis a determinadas funções, atividades, ou grupos profissionais.

No exercício das suas atividades, funções e competências, os colaboradores da empresa devem actuar, tendo em vista a prossecução dos interesses da empresa e no respeito pelos princípios da legalidade, boa fé, responsabilidade, transparência, lealdade, integridade, profissionalismo e confidencialidade, tendo em consideração a missão e as políticas de qualidade, de ambiente e de segurança em vigor. Estes princípios devem ser observados no relacionamento com qualquer entidade de regulação e supervisão, acionistas, clientes, fornecedores, prestadores de serviços, órgãos de comunicação social, entidades públicas e privadas, público em geral e nas relações internas entre colaboradores.

Os colaboradores não devem adotar comportamentos discriminatórios, em especial, com base na raça, sexo, idade, incapacidade física, orientação sexual, opiniões políticas ou convicções religiosas.

Os colaboradores da empresa devem cumprir sempre com zelo, eficiência e responsabilidade os encargos, deveres e equipamentos que lhes sejam cometidos no exercício das suas funções. D evem guardar absoluto sigilo e reserva em relação ao exterior de toda a informação de que tenham conhecimento no exercício das suas funções que, pela sua natureza, possa afetar a imagem, o interesse ou os negócios da empresa, afetar outros colaboradores ou clientes, em especial quando aquela seja de carácter confidencial.

Os colaboradores da empresa devem ter especial cuidado, nomeadamente com dados informáticos pessoais ou outros considerados reservados, informação sobre oportunidades de negócio ou negócios em curso, informação sobre competências técnicas, métodos de trabalho e de gestão de projetos desenvolvidos pela empresa, bem como a informação relativa a qualquer projeto realizado ou em desenvolvimento, cujo conhecimento esteja limitado aos colaboradores no exercício das suas funções ou em virtude das mesmas.

Os colaboradores da empresa não devem, em nome da empresa e no âmbito da sua atividade, violar a lei geral e a regulamentação específica aplicável. Devem ter especial atenção ao Regulamento Geral de Proteção de Dados Pessoais, que entrou recentemente em Vigor, devendo observar todos os princípios organizativos, tecnológicos e processuais em vigor neste domínio.

No âmbito das comunicações eletrónicas, os colaboradores da empresa devem restringir a utilização do email institucional a assuntos exclusivamente profissionais. Ainda no âmbito da utilização de equipamentos informáticos (computadores,

impressoras, internet e outros serviços e equipamentos empresariais), o acesso aos mesmos é regularmente monitorizado pela empresa, de forma a otimizar os mesmos. Em casos de caráter judicial, estes dados (incluindo os de localização física, acessos à internet, emails, videovigilância) podem vir a ser facultados às entidades competentes.

Incluir ou não cláusulas/aspectos relacionados com conflito de interesses, relações com terceiros, comunicação social, etc

Incluir ou não aspectos relacionados com penalizações por incumprimento, formas de comunicação de irregularidades, acompanhamento, entrada em vigor, etc.

b. Exemplos de políticas de privacidade para Websites:

https://termsfeed.com/blog/sample-privacy-policy-template/

https://www.nibusinessinfo.co.uk/content/sample-privacy-policy

https://privacypolicygenerator.info/

https://www.wikihow.com/Create-a-Website-Privacy-Policy

c. Exemplos de políticas de privacidade para envio de emails:

Exmo. Sr. Titulo Nome Apelido

(sempre que possível indicar o nome da pessoa a que nos dirigimos. Evitar envio de emails sem um destinatário perfeitamente identificado)

A proximidade e a relação de confiança que ao longo dos anos vimos a desenvolver com os nossos clientes, parceiros, colaboradores e fornecedores são fundamentais na missão e nas políticas da nossa empresa.

Para darmos continuidade a esta relação de proximidade, solicitamos o seu consentimento para lhe **enviarmos através desta via, e em conformidade com o novo RGPD**:

- Newsletters

- Convites para eventos

- Comunicados institucionais

- Ofertas e promoções comerciais

Desta forma, pedimos-lhe que siga este **link** para manifestar o seu consentimento.

Escolhendo não o fazer, este contacto será removido da nossa base de dados geral de comunicação, até 25 de maio. Apenas serão mantidos alguns dados pessoais em situações onde o relacionamento institucional ou comercial assim o exija por motivos legais (ex. NIF para efeitos de histórico de faturação durante o período definido na lei)

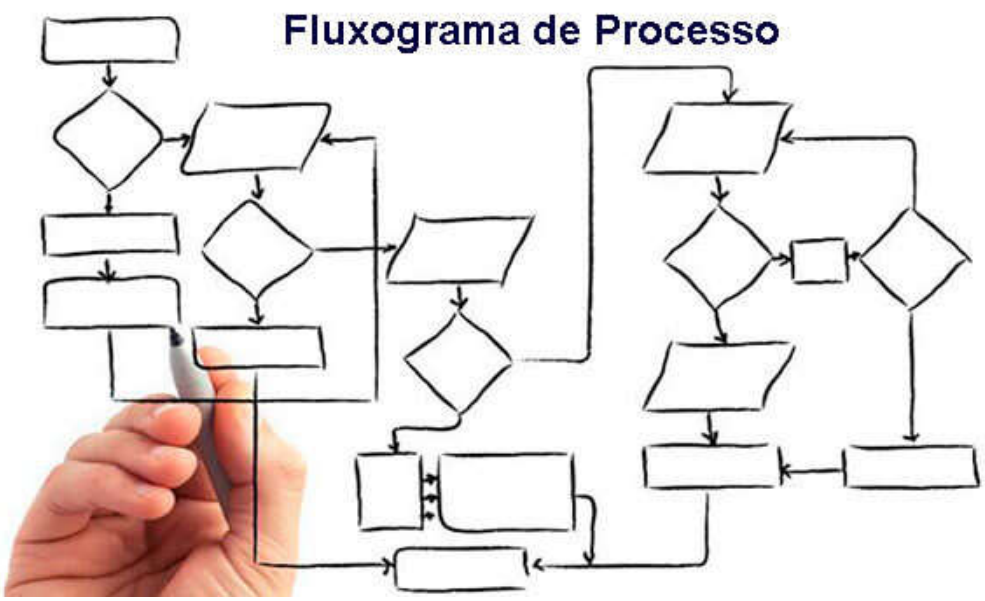
Caso dê o seu consentimento, ele pode ser sempre retirado, por si, a qualquer momento, através de contacto com a nossa área de gestão de dados pessoais (ex. protecao-dados@ciberseguranca.org)

Nota: Este pedido decorre da aplicação do novo regulamento europeu de proteção de dados pessoais (RGPD), que entra em vigor, a 25 de maio de 2018, bem como da nossa Política de Privacidade.

3. Exercício de direitos dos titulares de dados

O titular dos dados deve ser informado, nos termos do RGPD que lhe é garantido, a todo o tempo, o direito de acesso, retificação, atualização ou eliminação dos seus dados pessoais, bem como o direito de oposição ao tratamento dos mesmos, mediante pedido escrito dirigido à respetiva organização.

Recomenda-se que seja construído um fluxograma para documentar o processo relativo ao exercício dos direitos dos titulares dos dados, dentro da organização.



Identificar no fluxograma de processo, quem serão os intervenientes e quanto tempo têm para responder em cada ação/intervenção. O objetivo final é cumprir o prazo limite previsto no RGPD para tratamento dos pedidos dos titulares de dados (consultar secção 3 do RGPD).

Deve ainda ser definido o fluxograma de notificação de uma violação de dados pessoais à autoridade de controlo (artigo 33º e 34º RGPD)

4. Mecanismos de controlo e proteção de dados pessoais em vigor

Existem diversas formas de controlo de acesso a dados pessoais. Neste capitulo pretende-se documentar os controlos fiscos (limitações no acesso a espaços físicos que alojam ficheiros em papel ou equipamentos informáticos com informação digital).

a. Controlo físicos

Especificar que tipo de limitações existem (chaves, quem tem acesso, quem pode copiar, como limitar as cópias, como verificar se a politica de acesso está a ser cumprida, etc.)

b. Controlos lógicos (aplicações informáticas e dados digitais)

Especificar que tipo de limitações existem (restrições ao nível do IP, existência de passwords fortes (com mais de X caracteres, usando letras maiúsculas/minúsculas, caracteres especiais e números), quem tem acesso, quem pode imprimir ou exportar, como limitar as cópias, como verificar se a politica de acesso está a ser cumprida, etc.). No domínio digital, é muito importante perceber que é muito fácil realizar cópias de documentos e por vezes sem que haja registo dessa copia (ex. uma fotografia com o telemóvel ao próprio ecrã do computador).

c. Monitorização periódica

Quase tão importante como os controlos, é necessário implementar mecanismos de monitorização e *reporting*. Por exemplo, devem ser identificadas neste ponto as tecnologias que permitem identificar tentativas de acesso indevido ou apenas consultar o histórico de acesso. Esta manutenção periódica deve analisar os vários eventos, para que sejam tratados de acordo com a sua categoria (ex. tentativa de acesso indevido deve seguir um determinado procedimento, dado que é um evento que não devia existir e por isso deve ser analisado com maior urgência. Por outro lado, uma consulta a um histórico do acessos permitidos deve seguir outro procedimento)

Este capítulo depende muito do estágio de maturidade de cada organização e está intrinsecamente ligado ao capitulo seguinte, onde se identificam riscos e formas de minimização do impacto.

5. Riscos

Todas as organizações operam em contextos cada vez mais imprevisíveis e complexos, tornando-se fundamental abordar a questão do risco de uma forma consciente, planeada e sistematizada.

Embora não seja obrigatória que a nossa organização tenha um sistema de gestão de risco, é natural que qualquer ação, intervenção ou decisão seja acompanhada por uma avaliação de risco perfeitamente natural e automática. A "mentalidade de gestão de risco" está por isso presente em todas as decisões dos colaboradores, gestores, fornecedores e clientes. Cada decisão e ação, seja ao nível estratégico como operacional carece de uma avaliação de risco.

Numa ótica de gestão de dados pessoais, a nossa organização perguntar constantemente: "O que pode correr mal?" "Qual é a probabilidade disso acontecer?" "Quais são as consequências?" e "Como deveremos tratar este risco"?

Exemplo:

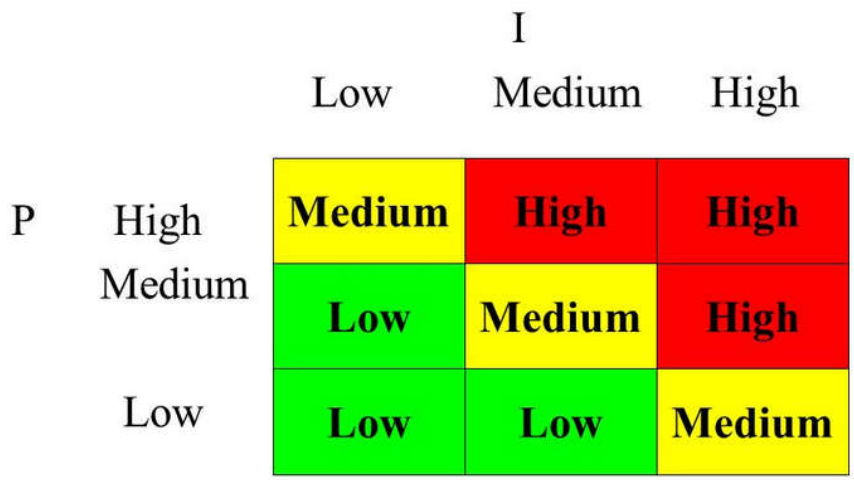
Risco	Probabilidade	Impacto	Fator Risco	Plano de Ação		
				O que pode ser feito para diminuir o impacto ou a probabilidade de vir a acontecer?	**Responsável**	**Próxima Data Verificação**
Desastres Naturais (ex. incêndio)				Arquivo externo à organização.		
Falhas em equipamentos				Política de backups e política de atualização de equipamentos informáticos		
Erros humanos involuntários				Política de backups e política de formação		
Erros na migração de dados de outros serviços				Dupla verificação		
Sabotagem				Política de monitorização de dados. Políticas de backups e reposição de dados.		
Acesso não autorizado a espaços físicos				Videovigilância e alarmística. Controlo de acessos com chaves ou mecanismos biométricos		

Colaboradores mal informados sobre as politicas de RGPD				Formação específica no regulamento geral de proteção de dados e mecanismos de proteção informática (ex. politicas de passwords fortes, não abrir emails de remetentes desconhecidos)		
Ataque externo, por tentativa de uso de passwords				Alertar os colaboradores para a necessidade de ter passwords com mais de X caracteres, com letras maiúsculas e minúsculas, caracteres especiais, etc.		
Servidores desatualizados				Implementar mecanismos de atualização automática. Políticas de verificação (ex. semanal, mensal, trimestral, etc.)		
Ataques internos (rede informática)				Monitorização da rede interna. Verificação e limitação de acessos através de redes Wifi pouco seguras.		
Vírus				Atualização dos sistemas de Antivírus		
Phishing				Formação específica no regulamento geral de proteção de dados e mecanismos de proteção informática (ex. politicas de passwords fortes, não abrir emails de remetentes desconhecidos)		
Roubo de informação				Formação específica no regulamento geral de proteção de dados e mecanismos de proteção informática (ex. politicas de passwords fortes, não abrir emails de remetentes desconhecidos)		
Ransomware				Política de monitorização de dados. Políticas de backups e reposição de dados.		
Espionagem				Formação específica no regulamento geral de proteção de dados e mecanismos de proteção informática (ex. politicas de passwords fortes, não abrir emails de remetentes desconhecidos)		
Negação de Serviços				Análise de tráfego na firewall e implementação de politicas de bloqueio automáticos.		
Corrupção de bases de dados ou ficheiros				Política de monitorização de dados. Políticas de backups e reposição de dados.		

Os riscos devem estar numerados, para depois ser mais fácil fazer o mapeamento com o plano de ações, plano de formação e plano de investimentos.

A forma de abordar o risco vai depender do contexto em que a organização opera. Para empresas que fornecem produtos e serviços simples, sem grandes implicações em termos de segurança ou financeiros, pode ser suficiente uma análise e priorização das suas atividades, de maneira a evitar problemas que poderiam afetar a satisfação do cliente. Para empresas atuando em áreas mais críticas esperar-se-ia uma abordagem mais abrangente (usando análises tipo FMEA, HAZOP, HACCP ou até metodologias estatísticas sofisticadas). A norma ISO 31010 oferece várias opções para análises de risco que poderiam ser aplicáveis em determinados contextos.

A ideia de ter uma classificação de risco, é definir prioridades nos investimentos e na monitorização e direcionar a nossa atenção. No exemplo acima é o resultado da matriz



Or, multiply PxI values, and decide thresholds.

23

A análise de risco permite não só evitar coisas más, mas aproveitar também as oportunidades para fazer melhor. Exemplo: uma nova tecnologia, uma matéria-prima mais barata, o concorrente com problemas,

O objetivo é que as organizações analisem os “riscos e oportunidades” de forma equilibrada, para que seu sistema possa alcançar os resultados pretendidos.

6. Oportunidades de Melhoria

Após identificação de todos os dados pessoais tratados na organização, identificada a licitude do seu tratamento, a localização dos mesmos, as politicas de privacidade, os riscos e contingências, é importante definir um plano de ação (seja na formação, seja em investimentos específicos, seja na reengenharia de processos) que permita elevar o nível de maturidade da organização no que respeita à gestão de informação (sejam dados pessoais, abrangidos pelo RGPD, sejam outros dados empresariais ou de negócio que nesta fase não estão abrangidos mas que são igualmente críticos para a organização).

a. Plano de Ações

O plano de ações da organização pode ser subdividido por unidades ou serviços, de acordo com a sua especificidade. Pode (e deve) ser revisto regularmente e devem ser emitidas novas versões sempre que seja adequado.

Devem ser identificados os riscos que se pretendem mitigar com cada uma das ações previstas (caso aplicável). Poderão existir ações a que não corresponde um risco específico assim como ações que pretendem dar resposta a vários riscos.

Exemplo:

Tratamento:					Responsável:				
Local:					Fonte: Plano de Ação		Emissão		
Observação									
Causa	O que (Descrição)	Quando (Prazo)	Quem (Responsáve	Porque (Justificativa)	Como (Detalhamento)	Onde (Local)	Custo	Eficácia	Status

b. Plano de formação

Numa ótica de melhoria contínua, a organização deve disponibilizar aos seus colaboradores um plano de formação e informação adequado à exigência e volatilidade do mundo global.

Da mesma forma, é aconselhável que se identifiquem os riscos que se pretendem mitigar com cada uma das formações previstas (caso aplicável). Poderão existir ações a que não corresponde um risco específico assim como ações que pretendem dar resposta a vários riscos.

Entre outras informações, devem ser registadas as ações de formação específicas, relacionadas com proteção e dados pessoais, a duração esperada, assim como o mês previsto.

7. **Exemplo:**

Ação de Formação	Objetivos	Duração	Horário	Local	Data Prevista									
					Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
		8 Horas	A Definir	A Definir										
		8 Horas	A Definir	A Definir										
		4 Horas	A Definir	A Definir										
		8 Horas	A Definir	A Definir										
		4 Horas	A Definir	A Definir										

c. Plano de investimento

Tal como referido anteriormente, é aconselhável que se identifiquem os riscos que se pretendem mitigar com cada um dos investimentos previstos (caso aplicável). Poderão existir investimentos a que não corresponde um risco específico assim como outros que pretendem dar resposta a vários riscos.

8. Conclusões

Este documento é apenas um template e deve ser ajustado à realidade de cada organização.

Da mesma forma, a conclusão depende de cada realidade. Porém, aconselha-se a que cubra alguns pontos essenciais:

- a informação é um ativo muito importante nas organizações

- a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamenta (pressuposto 1) do RGPD)

- a melhoria continua e o objetivo de conformidade total é um objetivo transversal à organização

- o cadastro e a documentação de sistemas e fontes de informação é fundamental para uma correta análise de risco

- a implementação de medidas de segurança e sua monitorização e algo que deve ser realizado com periodicidade

Recomenda-se na conclusão a referência a mais dois aspetos do RGPD:

d. DPO

Em termos gerais, o DPO é alguém dentro de uma empresa com capacidade para informar, aconselhar e orientar a direção da empresa bem como os seus trabalhadores a respeito das obrigações constantes do RGPD, assim como das outras disposições de proteção de dados em vigor na UE e noutros Estados Membros servindo ainda como o ponto de contacto da empresa com a autoridade de controlo nacional, que, em Portugal será a ser a Comissão Nacional de Proteção de Dados.

Existem situações em que deve ser designado obrigatoriamente um DPO para assegurar o cumprimento das novas regras em matéria de proteção de dados pessoais.

Nos termos do artigo 37.º do RGPD, deverá ser designado um DPO quando:

1. O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

2. As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

3. As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º

Deve ser referido, nas conclusões do documento, qual a decisão tomada pela organização:

Alternativa a) nomear um DPO responsável por todo o processo.

Alternativa b) Delegar no área de IT (ou outra a definir, ou num determinado profissional, interno ou contratado), a responsabilidade de gestão dos dados pessoais e demais funções normalmente atribuídas a um DPO.

e. DPIA

O artigo 35 deste regulamento apresenta o conceito de Avaliação de Impacto de Proteção de Dados (AIPD, em inglês Data Protection Impact Assessment – DPIA) que mais não é do que um processo pensado para descrever as metodologias e formas de registo, processamento, arquivo e transmissão de dados pessoais. Desta forma, avalia-se a necessidade e proporcionalidade de implementação de medidas que ajudem a identificar, minimizar ou eliminar os riscos para os direitos e liberdades de pessoas (individuais) resultantes do processamento de dados pessoais.

Os DPIAs não ser desenvolvidos e servir apenas para cumprir os requisitos do GDPR e evitar multas. Este documento é acima de tudo uma ferramenta para aproximar as áreas operacionais das áreas de gestão e aumentar a consciencialização do risco global dos dados tratados pela organização, responsabilizando todos os interveniente no processo. Para além da aproximação e responsabilização das estruturas (estratégicas e operacionais), o DPIA também é obviamente um instrumento de demonstração de que o RGPD está a ser cumprido em conformidade, aumentando a confiança dos clientes, fornecedores e entidades regulamentares.

Resumindo, um DPIA é um processo para construir, manter e demonstrar um elevado grau de conformidade e respeito pelos dados pessoais.

Na nossa organização decidiu-se :

Alternativa a) desenvolver um DPIA a partir deste documento, especificando com maior detalhe os níveis de risco e respetiva mitigação.

Alternativa b) Considerar que este documento é o DPIA , na medida em que face aos dados tratados todos os riscos estão devidamente identificados e considerados nos capítulos anteriores.

Finalizando, uma breve conclusão sobre este documento, sobre a periodicidade de revisão e sobre a forma de divulgação.

ANEXO 1 – Boas práticas de Segurança OWSAP

https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_Checklist

Input Validation

1. Conduct all data validation on a trusted system (e.g., The server)

2. Identify all data sources and classify them into trusted and untrusted. Validate all data from untrusted sources (e.g., Databases, file streams, etc.)

3. There should be a centralized input validation routine for the application

4. Specify proper character sets, such as UTF-8, for all sources of input

5. Encode data to a common character set before validating (Canonicalize)

6. All validation failures should result in input rejection

7. Determine if the system supports UTF-8 extended character sets and if so, validate after UTF-8 decoding is completed

8. Validate all client provided data before processing, including all parameters, URLs and HTTP header content (e.g. Cookie names and values). Be sure to include automated post backs from JavaScript, Flash or other embedded code

9. Verify that header values in both requests and responses contain only ASCII characters

10. Validate data from redirects (An attacker may submit malicious content directly to the target of the redirect, thus circumventing application logic and any validation performed before the redirect)

11. Validate for expected data types

12. Validate data range

13. Validate data length

14. Validate all input against a "white" list of allowed characters, whenever possible

15. If any potentially hazardous characters must be allowed as input, be sure that you implement additional controls like output encoding, secure task specific APIs and accounting for the utilization of that data throughout the application. Examples of common hazardous characters include: < > " ' % ( ) & + \ \' \"

16. If your standard validation routine cannot address the following inputs, then they should be checked discretely

Check for null bytes (%00)

Check for new line characters (%0d, %0a, \r, \n)

Check for “dot-dot-slash" (../ or ..\) path alterations characters. In cases where UTF-8 extended character set encoding is supported, address alternate representation like: %c0%ae%c0%ae/

(Utilize canonicalization to address double encoding or other forms of obfuscation attacks)

Output Encoding

17. Conduct all encoding on a trusted system (e.g., The server)

18. Utilize a standard, tested routine for each type of outbound encoding

19. Contextually output encode all data returned to the client that originated outside the application's trust boundary. HTML entity encoding is one example, but does not work in all cases

20. Encode all characters unless they are known to be safe for the intended interpreter

21. Contextually sanitize all output of un-trusted data to queries for SQL, XML, and LDAP

22. Sanitize all output of un-trusted data to operating system commands

Authentication and Password Management

23. Require authentication for all pages and resources, except those specifically intended to be public

24. All authentication controls must be enforced on a trusted system (e.g., The server)

25. Establish and utilize standard, tested, authentication services whenever possible

26. Use a centralized implementation for all authentication controls, including libraries that call external authentication services

27. Segregate authentication logic from the resource being requested and use redirection to and from the centralized authentication control

28. All authentication controls should fail securely

29. All administrative and account management functions must be at least as secure as the primary authentication mechanism

30. If your application manages a credential store, it should ensure that only cryptographically strong one-way salted hashes of passwords are stored and that the table/file that stores the passwords and keys is write-able only by the application. (Do not use the MD5 algorithm if it can be avoided)

31. Password hashing must be implemented on a trusted system (e.g., The server).

32. Validate the authentication data only on completion of all data input, especially for sequential authentication implementations

33. Authentication failure responses should not indicate which part of the authentication data was incorrect. For example, instead of "Invalid username" or "Invalid password", just use "Invalid username and/or password" for both. Error responses must be truly identical in both display and source code

34. Utilize authentication for connections to external systems that involve sensitive information or functions

35. Authentication credentials for accessing services external to the application should be encrypted and stored in a protected location on a trusted system (e.g., The server). The source code is NOT a secure location

36. Use only HTTP POST requests to transmit authentication credentials

37. Only send non-temporary passwords over an encrypted connection or as encrypted data, such as in an encrypted email. Temporary passwords associated with email resets may be an exception

38. Enforce password complexity requirements established by policy or regulation. Authentication credentials should be sufficient to withstand attacks that are typical of the threats in the deployed environment. (e.g., requiring the use of alphabetic as well as numeric and/or special characters)

39. Enforce password length requirements established by policy or regulation. Eight characters is commonly used, but 16 is better or consider the use of multi-word pass phrases

40. Password entry should be obscured on the user's screen. (e.g., on web forms use the input type "password")

41. Enforce account disabling after an established number of invalid login attempts (e.g., five attempts is common). The account must be disabled for a period of time sufficient to discourage brute force guessing of credentials, but not so long as to allow for a denial-of-service attack to be performed

42. Password reset and changing operations require the same level of controls as account creation and authentication.

43. Password reset questions should support sufficiently random answers. (e.g., "favorite book" is a bad question because “The Bible” is a very common answer)

44. If using email based resets, only send email to a pre-registered address with a temporary link/password

45. Temporary passwords and links should have a short expiration time

46. Enforce the changing of temporary passwords on the next use

47. Notify users when a password reset occurs

48. Prevent password re-use

49. Passwords should be at least one day old before they can be changed, to prevent attacks on password re-use

50. Enforce password changes based on requirements established in policy or regulation. Critical systems may require more frequent changes. The time between resets must be administratively controlled

51. Disable "remember me" functionality for password fields

52. The last use (successful or unsuccessful) of a user account should be reported to the user at their next successful login

53. Implement monitoring to identify attacks against multiple user accounts, utilizing the same password. This attack pattern is used to bypass standard lockouts, when user IDs can be harvested or guessed

54. Change all vendor-supplied default passwords and user IDs or disable the associated accounts

55. Re-authenticate users prior to performing critical operations

56. Use Multi-Factor Authentication for highly sensitive or high value transactional accounts

57. If using third party code for authentication, inspect the code carefully to ensure it is not affected by any malicious code

Session Management

58. Use the server or framework's session management controls. The application should only recognize these session identifiers as valid

59. Session identifier creation must always be done on a trusted system (e.g., The server)

60. Session management controls should use well vetted algorithms that ensure sufficiently random session identifiers

61. Set the domain and path for cookies containing authenticated session identifiers to an appropriately restricted value for the site

62. Logout functionality should fully terminate the associated session or connection

63. Logout functionality should be available from all pages protected by authorization

64. Establish a session inactivity timeout that is as short as possible, based on balancing risk and business functional requirements. In most cases it should be no more than several hours

65. Disallow persistent logins and enforce periodic session terminations, even when the session is active. Especially for applications supporting rich network connections or connecting to critical systems. Termination times should support business requirements and the user should receive sufficient notification to mitigate negative impacts

66. If a session was established before login, close that session and establish a new session after a successful login

67. Generate a new session identifier on any re-authentication

68. Do not allow concurrent logins with the same user ID

69. Do not expose session identifiers in URLs, error messages or logs. Session identifiers should only be located in the HTTP cookie header. For example, do not pass session identifiers as GET parameters

70. Protect server side session data from unauthorized access, by other users of the server, by implementing appropriate access controls on the server

71. Generate a new session identifier and deactivate the old one periodically. (This can mitigate certain session hijacking scenarios where the original identifier was compromised)

72. Generate a new session identifier if the connection security changes from HTTP to HTTPS, as can occur during authentication. Within an application, it is recommended to consistently utilize HTTPS rather than switching between HTTP to HTTPS.

73. Supplement standard session management for sensitive server-side operations, like account management, by utilizing per-session strong random tokens or parameters. This method can be used to prevent Cross Site Request Forgery attacks

74. Supplement standard session management for highly sensitive or critical operations by utilizing per-request, as opposed to per-session, strong random tokens or parameters

75. Set the "secure" attribute for cookies transmitted over an TLS connection

76. Set cookies with the HttpOnly attribute, unless you specifically require client-side scripts within your application to read or set a cookie's value

Access Control

77. Use only trusted system objects, e.g. server side session objects, for making access authorization decisions

78. Use a single site-wide component to check access authorization. This includes libraries that call external authorization services

79. Access controls should fail securely

80. Deny all access if the application cannot access its security configuration information

81. Enforce authorization controls on every request, including those made by server side scripts, "includes" and requests from rich client-side technologies like AJAX and Flash

82. Segregate privileged logic from other application code

83. Restrict access to files or other resources, including those outside the application's direct control, to only authorized users

84. Restrict access to protected URLs to only authorized users

85. Restrict access to protected functions to only authorized users

86. Restrict direct object references to only authorized users

87. Restrict access to services to only authorized users

88. Restrict access to application data to only authorized users

89. Restrict access to user and data attributes and policy information used by access controls

90. Restrict access security-relevant configuration information to only authorized users

91. Server side implementation and presentation layer representations of access control rules must match

92. If state data must be stored on the client, use encryption and integrity checking on the server side to catch state tampering.

93. Enforce application logic flows to comply with business rules

94. Limit the number of transactions a single user or device can perform in a given period of time. The transactions/time should be above the actual business requirement, but low enough to deter automated attacks

95. Use the "referer" header as a supplemental check only, it should never be the sole authorization check, as it is can be spoofed

96. If long authenticated sessions are allowed, periodically re-validate a user's authorization to ensure that their privileges have not changed and if they have, log the user out and force them to re-authenticate

97. Implement account auditing and enforce the disabling of unused accounts (e.g., After no more than 30 days from the expiration of an account's password.)

98. The application must support disabling of accounts and terminating sessions when authorization ceases (e.g., Changes to role, employment status, business process, etc.)

99. Service accounts or accounts supporting connections to or from external systems should have the least privilege possible

100. Create an Access Control Policy to document an application's business rules, data types and access authorization criteria and/or processes so that access can be properly provisioned and controlled. This includes identifying access requirements for both the data and system resources
Cryptographic Practices

101. All cryptographic functions used to protect secrets from the application user must be implemented on a trusted system (e.g., The server)

102. Protect master secrets from unauthorized access

103. Cryptographic modules should fail securely

104. All random numbers, random file names, random GUIDs, and random strings should be generated using the cryptographic module's approved random number generator when these random values are intended to be un-guessable

105. Cryptographic modules used by the application should be compliant to FIPS 140-2 or an equivalent standard. (See http://csrc.nist.gov/groups/STM/cmvp/validation.html)

106. Establish and utilize a policy and process for how cryptographic keys will be managed

Error Handling and Logging

107. Do not disclose sensitive information in error responses, including system details, session identifiers or account information

108. Use error handlers that do not display debugging or stack trace information

109. Implement generic error messages and use custom error pages

110. The application should handle application errors and not rely on the server configuration

111. Properly free allocated memory when error conditions occur

112. Error handling logic associated with security controls should deny access by default

113. All logging controls should be implemented on a trusted system (e.g., The server)

114. Logging controls should support both success and failure of specified security events

115. Ensure logs contain important log event data

116. Ensure log entries that include un-trusted data will not execute as code in the intended log viewing interface or software

117. Restrict access to logs to only authorized individuals

118. Utilize a master routine for all logging operations

119. Do not store sensitive information in logs, including unnecessary system details, session identifiers or passwords

120. Ensure that a mechanism exists to conduct log analysis

121. Log all input validation failures

122. Log all authentication attempts, especially failures

123. Log all access control failures

124. Log all apparent tampering events, including unexpected changes to state data

125. Log attempts to connect with invalid or expired session tokens

126. Log all system exceptions

127. Log all administrative functions, including changes to the security configuration settings

128. Log all backend TLS connection failures

129. Log cryptographic module failures

130. Use a cryptographic hash function to validate log entry integrity Data Protection:

131. Implement least privilege, restrict users to only the functionality, data and system information that is required to perform their tasks

132. Protect all cached or temporary copies of sensitive data stored on the server from unauthorized access and purge those temporary working files a soon as they are no longer required.

133. Encrypt highly sensitive stored information, like authentication verification data, even on the server side. Always use well vetted algorithms, see "Cryptographic Practices" for additional guidance

134. Protect server-side source-code from being downloaded by a user

135. Do not store passwords, connection strings or other sensitive information in clear text or in any non-cryptographically secure manner on the client side. This includes embedding in insecure formats like: MS viewstate, Adobe flash or compiled code

136. Remove comments in user accessible production code that may reveal backend system or other sensitive information

137. Remove unnecessary application and system documentation as this can reveal useful information to attackers

138. Do not include sensitive information in HTTP GET request parameters

139. Disable auto complete features on forms expected to contain sensitive information, including authentication

140. Disable client side caching on pages containing sensitive information. Cache-Control: no-store, may be used in conjunction with the HTTP header control "Pragma: no-cache", which is less effective, but is HTTP/1.0 backward compatible

141. The application should support the removal of sensitive data when that data is no longer required. (e.g. personal information or certain financial data)

142. Implement appropriate access controls for sensitive data stored on the server. This includes cached data, temporary files and data that should be accessible only by specific system users

Communication Security

143. Implement encryption for the transmission of all sensitive information. This should include TLS for protecting the connection and may be supplemented by discrete encryption of sensitive files or non-HTTP based connections

144. TLS certificates should be valid and have the correct domain name, not be expired, and be installed with intermediate certificates when required

145. Failed TLS connections should not fall back to an insecure connection

146. Utilize TLS connections for all content requiring authenticated access and for all other sensitive information

147. Utilize TLS for connections to external systems that involve sensitive information or functions

148. Utilize a single standard TLS implementation that is configured appropriately

149. Specify character encodings for all connections

150. Filter parameters containing sensitive information from the HTTP referer, when linking to external sites

System Configuration

151. Ensure servers, frameworks and system components are running the latest approved version

152. Ensure servers, frameworks and system components have all patches issued for the version in use

153. Turn off directory listings

154. Restrict the web server, process and service accounts to the least privileges possible

155. When exceptions occur, fail securely

156. Remove all unnecessary functionality and files

157. Remove test code or any functionality not intended for production, prior to deployment

158. Prevent disclosure of your directory structure in the robots.txt file by placing directories not intended for public indexing into an isolated parent directory. Then "Disallow" that entire parent directory in the robots.txt file rather than Disallowing each individual directory

159. Define which HTTP methods, Get or Post, the application will support and whether it will be handled differently in different pages in the application

160. Disable unnecessary HTTP methods, such as WebDAV extensions. If an extended HTTP method that supports file handling is required, utilize a well-vetted authentication mechanism

161. If the web server handles both HTTP 1.0 and 1.1, ensure that both are configured in a similar manor or insure that you understand any difference that may exist (e.g. handling of extended HTTP methods)

162. Remove unnecessary information from HTTP response headers related to the OS, web-server version and application frameworks

163. The security configuration store for the application should be able to be output in human readable form to support auditing

164. Implement an asset management system and register system components and software in it

165. Isolate development environments from the production network and provide access only to authorized development and test groups. Development environments are often configured less securely than production environments and attackers may use this difference to discover shared weaknesses or as an avenue for exploitation

166. Implement a software change control system to manage and record changes to the code both in development and production

Database Security

167. Use strongly typed parameterized queries

168. Utilize input validation and output encoding and be sure to address meta characters. If these fail, do not run the database command

169. Ensure that variables are strongly typed

170. The application should use the lowest possible level of privilege when accessing the database

171. Use secure credentials for database access

172. Connection strings should not be hard coded within the application. Connection strings should be stored in a separate configuration file on a trusted system and they should be encrypted.

173. Use stored procedures to abstract data access and allow for the removal of permissions to the base tables in the database

174. Close the connection as soon as possible

175. Remove or change all default database administrative passwords. Utilize strong passwords/phrases or implement multi-factor authentication

176. Turn off all unnecessary database functionality (e.g., unnecessary stored procedures or services, utility packages, install only the minimum set of features and options required (surface area reduction))

177. Remove unnecessary default vendor content (e.g., sample schemas)

178. Disable any default accounts that are not required to support business requirements

179. The application should connect to the database with different credentials for every trust distinction (e.g., user, read-only user, guest, administrators)

File Management

180. Do not pass user supplied data directly to any dynamic include function

181. Require authentication before allowing a file to be uploaded

182. Limit the type of files that can be uploaded to only those types that are needed for business purposes

183. Validate uploaded files are the expected type by checking file headers. Checking for file type by extension alone is not sufficient

184. Do not save files in the same web context as the application. Files should either go to the content server or in the database.

185. Prevent or restrict the uploading of any file that may be interpreted by the web server.

186. Turn off execution privileges on file upload directories

187. Implement safe uploading in UNIX by mounting the targeted file directory as a logical drive using the associated path or the chrooted environment

188. When referencing existing files, use a white list of allowed file names and types. Validate the value of the parameter being passed and if it does not match one of the expected values, either reject it or use a hard coded default file value for the content instead

189. Do not pass user supplied data into a dynamic redirect. If this must be allowed, then the redirect should accept only validated, relative path URLs

190. Do not pass directory or file paths, use index values mapped to pre-defined list of paths

191. Never send the absolute file path to the client

192. Ensure application files and resources are read-only

193. Scan user uploaded files for viruses and malware

Memory Management

194. Utilize input and output control for un-trusted data

195. Double check that the buffer is as large as specified

196. When using functions that accept a number of bytes to copy, such as strncpy(), be aware that if the destination buffer size is equal to the source buffer size, it may not NULL-terminate the string

197. Check buffer boundaries if calling the function in a loop and make sure there is no danger of writing past the allocated space

198. Truncate all input strings to a reasonable length before passing them to the copy and concatenation functions

199. Specifically close resources, don't rely on garbage collection. (e.g., connection objects, file handles, etc.)

200. Use non-executable stacks when available

201. Avoid the use of known vulnerable functions (e.g., printf, strcat, strcpy etc.)

202. Properly free allocated memory upon the completion of functions and at all exit points

General Coding Practices

203. Use tested and approved managed code rather than creating new unmanaged code for common tasks

204. Utilize task specific built-in APIs to conduct operating system tasks. Do not allow the application to issue commands directly to the Operating System, especially through the use of application initiated command shells

205. Use checksums or hashes to verify the integrity of interpreted code, libraries, executables, and configuration files

206. Utilize locking to prevent multiple simultaneous requests or use a synchronization mechanism to prevent race conditions

207. Protect shared variables and resources from inappropriate concurrent access

208. Explicitly initialize all your variables and other data stores, either during declaration or just before the first usage

209. In cases where the application must run with elevated privileges, raise privileges as late as possible, and drop them as soon as possible

210. Avoid calculation errors by understanding your programming language's underlying representation and how it interacts with numeric calculation. Pay close attention to byte size discrepancies, precision, signed/unsigned distinctions, truncation, conversion and casting between types, "not-a-number" calculations, and how your language handles numbers that are too large or too small for its underlying representation

211. Do not pass user supplied data to any dynamic execution function

212. Restrict users from generating new code or altering existing code

213. Review all secondary applications, third party code and libraries to determine business necessity and validate safe functionality, as these can introduce new vulnerabilities

214. Implement safe updating. If the application will utilize automatic updates, then use cryptographic signatures for your code and ensure your download clients verify those signatures. Use encrypted channels to transfer the code from the host server

ANEXO 2 – recomendações técnicas no Domínio da Cibersegurança

(fonte: Resolução do Conselho de Ministros n.o 41/2018)

Requisitos técnicos				
Requisito geral	**Requistos Específicos**			**Classificação**
As aplicações cliente (exemplo, Android, IOS, WEB) devem ser desenvolvidas adotando práticas de desenvolvimento seguro.	FE	1	Seguir as boas práticas de desenvolvimento. Exemplo: Open Web Application Security Project (OWASP), no que respeita ao desenvolvimento de código seguro e de submissão desse código a testes de segurança.	Obrigatório
		2	Utilização de sessões seguras com protocolo de Segurança.	Obrigatório
		3	Recomenda -se o uso de Transport Layer Security (TLS), na sua versão mais recente.	Recomendado
		4	Não guardar informação pessoal no browser, memória ou disco, para além do tempo da sessão e apenas na medida do necessário.	Obrigatório
	App	5	Utilização de sessões seguras com protocolo de Segurança.	Obrigatório
		6	Recomenda -se o uso de TLS, na sua versão mais recente, na comunicação com as camadas adjacentes.	Recomendado
		7	Se possível usar certificados através de Application Programming Interface (API), não sendo desta forma necessário o uso de palavras-passe.	Recomendado

		8	Não é permitida a utilização de credenciais em plain text, quer no código quer em ficheiros de configuração.	Recomendado
		9	Deve ser evitado palavras-passe embebidas no código.	Recomendado
		10	As credenciais que necessitem de ser armazenadas em ficheiros de configuração devem estar codificadas (HASH — mínimo SHA 256).	Recomendado
	BD	11	Comunicação com camada aplicacional através de autenticação por certificado válido por período não superior a 2 anos, no caso de as camadas serem física ou logicamente distintas. Exemplo: padrão X.509, da ITU-T para Infraestruturas de Chaves Públicas (ICP).	Obrigatório
		12	Prever cifra de informação pessoal (recomenda-se mínimo 2048 bit) apenas se a aplicação cliente tiver camada de BD física e logicamente distinta, usando preferencialmente tecnologia que permita interoperabilidade entre sistemas.	Obrigatório
Capacidade para autenticar e autorizar todos os	FE	13	O processo de autenticação deve ser sempre iniciado e mantido em sessão segura.	Obrigatório

utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações.		14	Recomenda -se: 1) o uso de TLS, na sua versão mais recente; ou 2) o uso de palavra -passe, preferencialmente em combinação com outro fator (Double Factor Authentication-2FA), como por exemplo: Palavra-passe + SMS Token Palavra-passe + Smartcard Palavra-passe + Biometria Palavra-passe + padrão gráfico Palavra-passe + Cartão de coordenadas Palavra-passe + código aleatório temporário (menos de 5 minutos de validade) enviado na forma de QR-Code	Recomendado
		15	Dados pessoais de sessão excluídos das variáveis Uniform Resource Locator (URL) ou de outras variáveis visíveis ao utilizador.	Obrigatório
		16	Credenciais de início de sessão transmitidos através do seu HASH, mínimo Secure Hash Algorithm-256 (SHA -256), ou utilização de cifra ou codificação para a transmissão de dados pessoais (nome do utilizador e palavra-passe em HASH e restantes dados cifrados).	Obrigatório

		17	Sempre que aplicável, a palavra-passe deve ter no mínimo 9 caracteres (13 caracteres para utilizadores com acesso privilegiado) e ser complexa. 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 (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório
		18	Recomenda-se que para novos sistemas seja sempre usado como padrão de autenticação o 2FA.	Recomendado
	App	19	A palavra -passe dos administradores deve ter no mínimo 13 caracteres e ser complexa. Neste caso, 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 (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ]: " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório
		20	Para todos os administradores deve-se utilizar Padrão de autenticação 2FA: Exemplos: Palavra-passe + Smartcard Palavra-passe + Biometria Palavra-passe + certificado (por exemplo X.509, da ITU -T para ICP, válido por período não superior a 2 anos).	Obrigatório

		21	Como mecanismo de proteção e segurança da informação recomenda-se o uso de Token.	Recomendado
		22	Comunicação com camadas FE ou BD através de sessão segura, com prévia autenticação se camadas forem física ou logicamente distintas.	Obrigatório
		23	Deve ser evitado palavras-passe embebidas no código. Quando tal não for possível, devem estar codificadas (HASH, mínimo SHA -256).	Recomendado
		24	Se possível, usar certificados através de API, não sendo desta forma necessário o uso de palavras-passe.	Recomendado
		25	Autenticação de elementos comunicantes garantida por validação de informação estática ao nível da rede. Exemplos: 1) utilização de IP fixo + hostname + MacAddress + fatores de autenticação, ou 2) Utilização de certificados	Obrigatório
	BD	26	A palavra -passe deve ter no mínimo 13 caracteres e ser complexa. Neste caso, 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 (~ ! @ # $ % ^ & *( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório
		27	Dados pessoais de autenticação, transmitidos através do seu HASH (mínimo SHA-256), ou recorrendo à cifra ou codificação para efetuar essa transmissão.	Recomendado

Atribuição de direitos de acesso e rivilégio de forma restrita e controlada.	FE	28	Criação de perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (Create, Read, Update, Delete — CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		29	Criação de registo de acesso, alteração e remoção (logs), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório
	App	30	Criação perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		31	Criação de registo de acesso, alteração e remoção (logs) com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório
	BD	32	Criação perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		33	Criação de registo de acesso, alteração e remoção (logs), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório
Atribuição das credenciais de acesso de forma	FE	34	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório

controlada através de um processo formal de gestão do respetivo ciclo de vida.		35	Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação. Exemplo: Envio de informação de autenticação por SMS com validade limitada (não superior a 5 minutos), com primeiro acesso a implicar sempre a redefinição da informação enviada; Envio de informação de autenticação gerada automática e aleatoriamente, enviada por Envelope (semelhante ao do envio de dados do Cartão de Cidadão).	Obrigatório
	App	36	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório
		37	Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação.	Obrigatório
	BD	38	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório
		39	Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação.	Obrigatório
Revisão de direitos de acesso de utilizadores em intervalos regulares.	FE	40	Processo de renovação de conta do utilizador de acordo com os mesmos requisitos de segurança da criação do mesmo, não devendo ter um ciclo de vida superior a 180 dias.	Obrigatório

		41	A gestão do ciclo de vida da conta do utilizador deve ter em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		42	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
		43	Deve ser desativada uma conta de utilizador quando o mesmo não tem atividade sobre a conta durante 3 meses	Recomendado
	App	44	Processo de gestão de validade de perfis.	Obrigatório
		45	Processo de gestão de validade de perfis automatizado.	Recomendado
		46	Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório
		47	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
	BD	48	Processo de gestão de validade de perfis.	Obrigatório
		49	Processo de gestão de validade de perfis automatizado.	Recomendado

		50	Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório
		51	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados.	FE	52	A gestão do ciclo de vida da conta do utilizador deve ter em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta de utilizador é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		53	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
		54	Ação dos utilizadores sobre dados pessoais (CRUD) deve permitir a sua auditoria em registo de atividade (logs).	Obrigatório
	App	55	Para Administradores de Sistemas, Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório
		56	Processo de gestão de validade de contas de utilizadores.	Obrigatório
		57	Processo de gestão de validade de contas de utilizadores automatizado.	Recomendado

		58	Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade limitada.	Obrigatório
		59	Recomenda -se: 1) uma periodicidade bimestral; ou 2) quando se verifique uma alteração no mapa de pessoal associado a esta função.	Recomendado
		60	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
	BD	61	Para Administradores de Bases de Dado, Administradores de Sistemas, de Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório
		62	Processo de gestão de validade das contas dos utilizadores.	Obrigatório
		63	Processo de gestão de validade das contas dos utilizadores automatizado.	Recomendado
		64	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
Restrição de acesso à informação baseado no princípio necessidade de conhecer (criação de perfil).	FE	65	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório

	App	66	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		67	Processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório
	BD	68	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		69	Processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório
Automatização dos processos de concessão, revisão, análise e revogação de acesso.		70	Aplicam -se as mesmas disposições que em «Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados» e «Revisão de direitos de acesso de utilizadores em intervalos regulares».	Obrigatório
Procedimentos seguros de início de sessão.		71	Aplicam -se as mesmas disposições referidas em «Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o acesso controlado por um procedimento seguro de início de sessão».	Obrigatório

Capacidade de monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis.		72	Deve ser guardado registo de atividade (log) de todas as ações que um utilizador efetue sobre dados pessoais, independentemente do seu perfil e função.	Obrigatório
		73	Todos os registos de atividade (log) devem ser armazenados apenas em modo de leitura, devendo, com uma periodicidade máxima de 1 mês, ser englobados num único bloco de registos e assinado digitalmente (garantia de integridade).	Obrigatório
		74	Deve ser guardado registo de atividade (log) de todos os acessos e tentativas falhadas de acesso, obedecendo aos requisitos anteriores.	Obrigatório
		75	Garantir que os registos de atividade provenientes dos diversos subsistemas (Sistemas Operativos, aplicações, browsers, Sistema de Gestão de Base de Dados — SGBD, etc.) são inequivocamente associados à sua origem.	Obrigatório
		76	Os registos de atividade (log) devem conter, no mínimo, o endereço de acesso (IP e Porto), Host, HASH da conta do utilizador que efetuou a ação, ação efetuada (CRUD), Tipo de Dado Pessoal onde a ação foi efetuada, data/hora/minuto/segundo (TimeStamp) da ação, alteração efetuada sobre o dado pessoal.	Obrigatório

Inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional.		77	Tendo em vista garantir que a entidade responsável pelo tratamento de dados deve definir e implementar mecanismos de proteção da informação em função da sua relevância e criticidade, deve ser implementado: Deteção de ameaças na defesa perimétrica do sistema (por exemplo, regras definidas nas firewall, Intrusion Detection System — IDS, etc.); Extensão desta proteção desejavelmente a todos os dispositivos (incluindo móveis) com acesso a dados pessoais nos sistemas corporativos; Mecanismo de cifra ponto a ponto sempre que houver necessidade de aceder remotamente ao FE (e apenas a esta camada), como por exemplo com recurso à tecnologia Virtual Private Network (VPN).	Obrigatório
Proteção dos dados contra modificações não autorizadas, perdas, furtos e divulgação não autorizada.	FE	78	FE desenvolvido e em produção de acordo com as melhores práticas de segurança, garantindo a proteção desta camada aos ataques mais comuns (SQLi, injeção de código, etc.).	Obrigatório
		79	Recomenda -se as práticas recomendadas em Open Web Application Security Project (OWASP).	Recomendado
		80	Aplicam -se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório
	App	81	Camada aplicacional segregada da rede ou ambiente com visibilidade e/ou acesso exterior.	Obrigatório
		82	Aplicam -se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório

	BD	83	Camada de BD segregada da rede ou ambiente com visibilidade/acesso exterior.	Obrigatório
		84	Aplicam -se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório
		85	Mascaramento, anonimização ou, sendo necessário, cifra dos dados pessoais transmitidos ou acedidos.	Obrigatório
		86	Dados armazenados (incluindo os existentes em volumes de salvaguarda — backups) devem ser cifrados e assinados digitalmente.	Recomendado
		87	Recomenda -se que, para dados pessoais considerados muito críticos, o seu armazenamento seja efetuado de forma fragmentada e em locais físicos distintos, mantendo -se todavia a sua unicidade e integridade lógica.	Recomendado
Capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados pessoais.		88	Deve ser garantida a integridade das zonas Domain Name System (DNS) onde se encontra inserido o sistema e o ecossistema envolvente, recorrendo às boas práticas de DNSSec e de configuração de sistemas de Correio Eletrónico (por exemplo, Sender Policy Framework — SPF, DomainKeys Identified Mail — DKIM, Domain -based Message Authentication, Reporting and Conformance — DMARC, entre outros).	Obrigatório
		89	Deve ser utilizada tecnologia de comunicação segura (por exemplo VPN), com sistema de autenticação forte (preferencialmente através de certificados), para que a transmissão de dados entre entidades de ambientes tecnológicos distintos seja efetuada em segurança.	Recomendado

Os sistemas de armazenamento devem garantir redundância e disponibilidade, não devendo existir nenhum «single point of failure».		90	A arquitetura de processamento e armazenamento deve garantir as propriedades da redundância, resiliência e disponibilidade.	Obrigatório
		91	Devem existir dois tipos de backups (online e offsite), que devem obedecer aos mesmos requisitos de segurança definidos para os sistemas produtivos.	Obrigatório
		92	Os backups offsite devem ser guardados numa localização que não esteja exposta aos mesmos riscos exteriores da localização original, podendo ser da organização mas geograficamente distinta e/ou afastada.	Obrigatório
As redes e sistemas de informação devem possuir as funcionalidades necessárias ao respeito pelos direitos do titular dos dados.		93	Os sistemas devem estar capacitados para classificar, priorizar, pesquisar, editar e apagar os dados pessoais.	Obrigatório
		94	Os sistemas devem possuir os controlos necessários que permitam a identificação, autenticação, acesso e validação dos dados pessoais armazenados.	Obrigatório
As tecnologias de informação a implementar devem permitir a portabilidade e a exportação de dados pessoais.		95	Deve -se garantir a utilização de formatos digitais compatíveis, que assegurem a interoperabilidade técnica e semântica dentro da Administração Pública, na interação com o cidadão ou com a empresa e para disponibilização de conteúdos e serviços, adotando as especificações técnicas e formatos digitais definidos no Regulamento Nacional de Interoperabilidade Digital, aprovado pela Resolução do Conselho de Ministros n.º 91/2012, ou noutro que o venha a substituir.	Obrigatório

Devem ser definidas políticas que garantam a segurança dos dados pessoais, em alinhamento com a estratégia superiormente definida para a segurança do tratamento de dados pessoais.		96	As políticas que garantam a segurança do tratamento de dados pessoais devem abranger: A priorização e classificação dos dados de acordo com os critérios de sensibilidade e criticidade predefinidos; A criação; A modificação; A transmissão; A recolha (independentemente do respetivo meio ou processo); A destruição; O armazenamento (incluindo a retenção); A pesquisa de dados.	Obrigatório
		97	Deve -se garantir o conhecimento, a todo o tempo, dos ativos de informação relativamente a dados pessoais, de modo a permitir identificar inequivocamente o estado da informação em todo o seu ciclo de vida.	Obrigatório