



MUNICÍPIO DE VILA VELHA DE RÓDÃO

CÂMARA MUNICIPAL

Aprovado,

O Presidente da Câmara Municipal,


04-04-2022

CADERNO DE ENCARGOS

**AQUISIÇÃO DE SERVIÇOS DE COMUNICAÇÕES, ALOJAMENTO DE CAIXAS DE
E-MAIL, SERVIDORES VIRTUAIS E ALUGUER DE EQUIPAMENTOS**

PARTE I

Cláusulas Jurídicas

Artigo 1.º

Entidade pública contratante

A entidade pública contratante é o Município de Vila Velha de Ródão, pessoa coletiva 506642798 sito na Rua de Santana 6030-230 Vila Velha de Ródão, com o número de telefone 272540300, de fax 272540301 e com o e-mail geral@cm-vvrodão.pt.

Artigo 2.º

Objeto

O objeto do procedimento consiste, de acordo com as especificações técnicas descritas na Parte II do presente Caderno de Encargos, **na aquisição de serviços de comunicações, alojamento de caixas de e-mail, servidores virtuais e aluguer de equipamentos.**

Artigo 3.º

Local da entrega

Os serviços e equipamentos objeto deste contrato deverão ser **prestados/entregues e acessíveis nas instalações da entidade adjudicante**, ou seja, nos diversos edifícios da Câmara Municipal no concelho de Vila Velha de Ródão.

Artigo 4.º

Prazo de entrega

A entrega dos equipamentos e a operacionalização dos serviços a realizar no âmbito do presente contrato deverão ser integralmente executados no prazo máximo de **20 dias úteis a contar da assinatura do contrato.**

Artigo 5.º

Condições de pagamento

1. O aluguer e serviços prestados no âmbito do presente contrato deverão ser **faturados mensalmente** no mês seguinte ao da sua efetiva prestação, sendo o pagamento efetuado num **prazo de 30 dias** relativamente à data de emissão da fatura.
2. Em caso de discordância por parte da **entidade adjudicante**, quanto aos valores indicados nas faturas, deverá este comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.

Artigo 6.º

Valor

1. Pela prestação de serviços e aluguer objeto do presente procedimento, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a entidade adjudicante deve pagar ao adjudicatário **o preço constante da proposta adjudicada**, que se estima ser **52.292,90€** (cinquenta e um dois mil, duzentos e noventa e dois euros e noventa centimos) acrescido de IVA à taxa legal em vigor;
2. O preço referido inclui:
 - a) 24 Prestações mensais fixas **não superiores a 1.778,87€**, devidas pela prestação dos serviços e pelo aluguer dos equipamentos, estimando-se 1.578,54€ pela prestação dos serviços e 200,33€ pelo aluguer dos equipamentos;

- b) 24 Prestações mensais variáveis devidas pelas comunicações/serviços extra, que se estimam **ser 400,00€**. Estas comunicações/serviços estão previstas e, como tal, definidas nas Especificações Técnicas, Parte II do presente Caderno de Encargos.
- 3. Os preços referidos nos números anteriores incluem todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante.
- 4. O montante estimado referido nos números 1 e 2 do presente artigo que deve considerar-se o preço base, nos termos do art.º 47 do CCP como montante máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o objeto do procedimento.

Artigo 8.º

Obrigações do adjudicatário

- 1. O adjudicatário obriga-se a cumprir os requisitos e obrigações constantes das especificações técnicas descritas na parte II do presente Caderno Encargos e de acordo com o prazo referido no artigo 4º.
- 2. O adjudicatário obriga-se a cumprir as garantias e suportes conforme previsto no artigo 14º.
- 3. O adjudicatário obriga-se a faturar mensalmente, no mês seguinte ao da prestação.

Artigo 9.º

Obrigações do adjudicante

- 1. A entidade adjudicante compromete-se, através dos seus serviços, a fornecer todo o apoio necessário ao adjudicatário, para a prestação de serviços das soluções propostas por este;
- 2. Disponibilizar as condições físicas, materiais e humanas necessárias ao correto funcionamento dos sistemas propostos;
- 3. A entidade adjudicante compromete-se a pagar as faturas dentro do prazo.

Artigo 10.º

Contrato

- 1. O procedimento dará lugar a contrato escrito, que será assinado pelos outorgantes na plataforma de contratação eletrónica, onde decorre o procedimento;
- 2. O Contrato é composto pelo respetivo clausulado contratual e os seus anexos;
- 3. Fazem parte integrante do contrato os seguintes documentos:
 - a) Os esclarecimentos e as retificações relativas ao caderno de encargos;
 - b) O caderno de encargos;
 - c) A proposta adjudicada;
 - d) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
- 4. Em caso de dúvida ou divergência entre os documentos referidos no n.º 2, a prevalência é determinada pela ordem pela qual são indicados nesse número.

Artigo 11.º

Objeto do dever de sigilo

- 1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à entidade adjudicante, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato;
- 2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato;

3. Exclui-se o dever de sigilo previsto na informação e na documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que este esteja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou de outras entidades administrativas competentes.

Artigo 12.º

Duração do contrato

1. O contrato inicia-se com a assinatura do mesmo e termina 24 meses depois, independentemente de não ter sido atingido o valor total previsto no n.º 1 do artigo 6.º.
2. O contrato terminará igualmente logo que seja atingido o valor previsto no n.º 1 do artigo 6.º ainda que não tenham decorrido os 24 meses atrás referidos.

Artigo 13.º

Penalidades

1. No caso de incumprimento dos prazos fixados no artigo 4.º para o **fornecimento de equipamentos e a operacionalização dos serviços** por causa imputável ao adjudicatário, poderá ser-lhe aplicada uma penalidade, calculada de acordo com a seguinte fórmula: $P = V \times A/75$, em que:
P corresponde ao montante da penalidade;
V corresponde ao valor da mensalidade a pagar;
A corresponde ao número de dias em atraso.
2. No caso de incumprimento no **fornecimento dos serviços** por período superior ao previsto no n.º 2 e n.º 3 do artigo 14.º, aplicar-se-á uma penalização de 100% sobre o valor dos serviços inoperacionais.

Artigo 14.º

Garantias e suporte

1. Todos **equipamentos propostos deverão ser identificados pela respetiva marca e modelo** e, no período de vigência do contrato, **deverão estar cobertos** pela garantia;
2. Em caso de falha ou avaria de equipamentos, a sua **reparação ou substituição** deverá ser efetuada **nas instalações da entidade adjudicante sem custos extra**.
3. Pelos serviços e aluguer de equipamentos do presente procedimento, o concorrente deverá **apresentar os respetivos SLA (Service Level Agreement)**, sendo que, os mesmos deverão **enquadrar-se nos valores de referência** do mercado para cada item.

Artigo 15.º

Casos fortuitos ou de força maior

1. Não podem ser impostas penalidades ao prestador de serviços, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Podem constituir motivos de força maior, caso se venha a verificar os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

3. Não constituem força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do prestador de serviços ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Artigo 16.º

Comunicações e notificações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma das partes identificada no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Artigo 17.º

Resolução de litígios - Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal de Castelo Branco.

Artigo 18.º

Proteção de dados pessoais

O adjudicatário obriga-se a cumprir a Lei de Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro), ou diploma legal que sobrevier, o Regulamento Geral sobre a Proteção de Dados (Regulamento EU 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016), assim como, o Anexo RGPD do presente Caderno de Encargos.

Artigo 19.º

Legislação aplicável

O procedimento é regulado pela legislação portuguesa, nomeadamente o Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro na redação do Decreto-lei n.º 111-B/2017 de 31 de agosto e legislação conexas.

PARTE II

Especificações Técnicas

O adjudicatário deverá **fornecer serviços de comunicações, alojamento de caixas de e-mail, servidores virtuais e aluguer de equipamentos** de acordo com as características apresentadas de seguida. Este fornecimento divide-se em quatro vertentes:

- Equipamentos e serviços para redes fixas, ligações e conectividade internet e plataforma web de envio de SMS;
- Caixas de correio eletrónico;
- Equipamentos e serviços de voz e internet para rede móvel;
- Servidores virtuais privados, serviços, comunicações e equipamentos.

Para cada uma das vertentes o concorrente **deverá apresentar o preço fixo mensal**, sendo que, está previsto/reservado um **custo em comunicações/serviços variáveis** no valor de **400,00€/mês**. O concorrente deverá incluir este valor no somatório das parcelas da mensalidade, assim sendo, já com o custo em comunicações/serviços variáveis incluído, as **prestações mensais deverão ter um valor não superior a 2.178,87€**.

São consideradas **comunicações/serviços variáveis**:

- As chamadas efetuadas através da rede fixa para as redes móveis, números especiais e estrangeiro; as SMS enviados extra *plafond* mensal; as chamadas recebidas no número verde;
- Através da rede móvel, as chamadas/SMS/tráfego internet realizadas após esgotado o pacote de minutos/SMS/Megabytes mensais; e os tráfegos extra *plafond* mensal consumidos nas bandas largas móveis;
- Outros recursos extra, consumidos além dos definidos como base do presente procedimento.

O adjudicatário deverá **ativar todos serviços**, realizar as **configurações iniciais** e ministrar **formação** aos utilizadores sem nenhum custo adicional.

O adjudicatário deverá ter **disponível 24 horas por dia** uma linha telefónica para suporte aos serviços contratados e aos equipamentos alugados, bem como **designar um gestor dedicado** para servir de interlocutor com a entidade adjudicante.

De seguida serão detalhadas cada uma das vertentes referidas. Sempre que se justifique, **será apresentado o preço máximo aceite** pela entidade adjudicante para efeitos do presente fornecimento.

1. Equipamentos e serviços para redes fixas, ligações e conectividade internet e plataforma de envio de SMS

1.1. Conetividades e acesso internet

- **1 (uma) ligação através de fibra ótica Gigabit Ethernet 1000BaseT**, com robustez e capacidade para múltiplas conexões simultâneas através desta (desde que o somatório das diversas capacidades não ultrapasse o limite de 1Gbps), incluindo todo o equipamento e respetivo suporte técnico. A marca/modelo do equipamento de suporte desta ligação deverá ser referida pelo concorrente de modo a comprovar a robustez necessária para garantir a mesma, sendo que, o Router NTE deverá possuir características mínimas equivalentes ou superiores ao equipamento Teldat M8Smart. Esta ligação deverá ser instalada na seguinte localização:

Edifício dos Paços do Concelho
Rua Santana, 6030-230 Vila Velha de Ródão

Coordenadas: 39°39'28.8"N 7°40'35.6"W

- **1 (uma) conectividade internet 300/300Mbps através da ligação Gigabit Ethernet do ponto anterior**, sem contenção, com IP Fixo e tráfego ilimitado. Adicionalmente, sobre esta conectividade a entidade adjudicante vai realizar um pedido de atribuição de endereçamento IPv4 público, num máximo de 16 endereços IP, sem custos extra associados.
- **2 (dois) pacotes de acesso internet, voz e TV através de rede Gigabit Passive Optical com performance de 1000/200Mbps**, com BOX de TV e 150 canais, tráfego ilimitado, chamadas grátis para as redes fixas nacionais e incluindo todo o equipamento e respetivo suporte técnico. O equipamento telefónico não será necessário. Estas ligações deverão ser instaladas nas seguintes localizações:

Edifício dos Paços do Concelho

Rua Santana, 6030-230 Vila Velha de Ródão

Coordenadas: 39°39'28.8"N 7°40'35.6"W

Piscina de Fratel

Rua Inspector José Batista Martins, 6030-012 Fratel

Coordenadas: 39°37'54.6"N 7°44'45.9"W

- **1 (um) pacote de acesso internet, voz e TV através de rede Gigabit Passive Optical com performance de 100/100Mbps**, com BOX de TV e 150 canais, tráfego ilimitado, chamadas grátis para as redes fixas nacionais e incluindo todo o equipamento e respetivo suporte técnico. O equipamento telefónico não será necessário. Esta instalação deverá contemplar a portabilidade do número 272541098. Esta ligação deverá ser instalada na seguinte localização:

Ginásio Municipal

Rua Comendador João Martins, 6030-242 Vila Velha de Ródão

Coordenadas: 39°39'07.4"N 7°40'04.4"W

- **1 (um) pacote de acesso internet e voz através de rede Gigabit Passive Optical com performance de 1000/200Mbps**, tráfego ilimitado, chamadas grátis para as redes fixas nacionais e incluindo todo o equipamento e respetivo suporte técnico. O equipamento telefónico não será necessário. Esta ligação deverá ser instalada na seguinte localização:

Praia Fluvial da Foz do Cobreão

Rua do pontão 7A, Foz do Cobreão, 6030-155 Vila Velha de Ródão

Coordenadas: 39°43'48.8"N 7°45'38.1"W

- **1 (um) pacote de acesso internet, voz e TV através de rede ADSL com performance de 16/1Mbps**, com BOX de TV e 150 canais, tráfego ilimitado, chamadas grátis para as redes fixas nacionais e incluindo todo o equipamento e respetivo suporte técnico. O equipamento telefónico não será necessário. Esta ligação deverá ser instalada na seguinte localização:

Centro de Convívio de Sarnadas de Ródão

Rua da Escola 6, 6030-111 Sarnadas de Ródão

Coordenadas: 39°44'54.0"N 7°37'33.7"W

1.2. Serviços de voz fixa

- **20 (vinte) DDI's** (números 272540300 ao 272540319).
- Incluir na rede de voz o **número verde 800 20 28 29**, com capacidade para aceder a todas as facilidades da restante rede interna. Máximos preços por minuto admitidos em chamadas com origem em redes fixas ou móveis nacionais: 0,035€/minuto (+IVA). Com faturação ao segundo após o 1º minuto e sem taxas de ativação de chamada.
- As comunicações da **rede interna** devem ter **chamadas gratuitas para todas as redes fixas nacionais**.

- O concorrente deve apresentar o preço para as comunicações da rede interna, que devem ter **0,04€ (+IVA) de preço máximo admitido por minuto para qualquer rede móvel de Portugal**. Com faturação ao segundo após o 1º minuto e sem taxas de ativação de chamada.
- As comunicações da rede interna devem ter **preços por minuto para comunicações internacionais** enquadradas com os valores de referência do mercado. O concorrente deverá apresentar estes preços detalhadamente.
- **6 (seis) Linhas analógicas telealimentadas em circuito de cobre** para instalar em equipamentos de segurança nos edifícios do Município em Vila Velha de Ródão. Equipamento telefónico não necessário. Estas linhas devem **incluir 500 minutos mensais de chamadas para as redes fixas nacionais e 100 minutos mensais de chamadas para redes móveis nacionais**. Para as comunicações extra, o concorrente deverá apresentar os preços. A sua localização é a seguinte:

Biblioteca Municipal José Batista Martins

Rua Santana 496, 6030-230 Vila Velha de Ródão

Coordenadas: 39°39'19.8"N 7°40'27.1"W

Casa de Artes e Cultura do Tejo

Rua Santana 459, 6030-230 Vila Velha de Ródão

Coordenadas: 39°39'18.5"N 7°40'28.6"W

Escola Básica de Vila Velha de Ródão

Av. da Bela Vista, 6030-201 Vila Velha de Ródão

Coordenadas: 39°39'12.9"N 7°40'38.2"W

Jardim de Infância de Vila Velha de Ródão

Caminho Agrícola da Cova do Rodão, Vila Velha de Ródão

Coordenadas: 39°39'20.3"N 7°40'08.5"W

Edifício da ADRACES em Vila Velha de Ródão

Rua Santana 277, 6030-230 Vila Velha de Ródão

Coordenadas: 39°39'14.0"N 7°40'24.5"W

Estádio Municipal de Vila Velha de Ródão

Rua José Baptista Martins, 6030-223 Vila Velha de Ródão

Coordenadas: 39°39'05.1"N 7°39'50.8"W

1.3. Fax online

Serviço de gestão documental **Fax-to-Email e Email-to-Fax** mantendo o número de fax atual 272540301.

1.4. Central telefónica virtual

Pretende-se a implementação de uma solução que **não inclua o equipamento tradicional** nas instalações da entidade adjudicante. Deverá permitir **total convergência ente as comunicações de voz fixas e móveis sem custos nas mesmas**. Deve possuir as seguintes características mínimas:

- **67** (sessenta e sete) **utilizadores de central telefónica virtual**;
- **16** (desaseis) **canais**;
- Possibilidade de expansão para um número de canais superior sem alterações estruturais;
- **Múltiplos reencaminhamentos** com modulação temporal;
- **Administração remota** através de plataforma web;
- Música e voz de espera configuráveis;
- Possibilidade Serviços de **IVR**;
- Configuração de múltiplos horários de atendimento;
- Possibilidade de ter **extensões fora do escritório**;
- Possibilidade de configurar **“grupos de toque”**;

- Funcionalidades de **remarcação, rejeição e redirecionamento de chamadas**;
- Modulação horária para restrições de chamadas;
- **Captação seletiva, estacionamento e conferência de chamadas**;
- **Marcação direta às extensões e mãos livres**.

1.5. Plataforma de envio de SMS

Para enviar mensagens SMS com divulgação de informação da entidade adjudicante para contactos telefónicos existentes em base de dados, o concorrente deverá apresentar proposta para:

- Fornecimento de **plataforma web para envio de SMS**;
- **3000** (três mil) **SMS mensais incluídas no tarifário**;
- As SMS mensais não utilizados **deverão acumular** para os meses seguintes, expirando apenas em ciclos anuais do contrato;
- Preço unitário máximo admitido das SMS excedentes: 0,035€ (+IVA).

1.6. Aluguer de equipamentos

Sendo a rede interna composta por 67 posições, o concorrente deverá apresentar proposta para o aluguer dos seguintes equipamentos:

1 (um) Telefone avançado IP para Operadora + 4 (quatro) módulos de expansão com capacidade para integrar as posições da rede interna, com as seguintes características mínimas:

- 480x272 TFT LCD a cores com 6 linhas;
- LCD de 4.3”;
- 5 teclas programáveis sensíveis ao contexto;
- 24 teclas programáveis de extensão BLF;
- Dupla porta de rede Gigabit;
- Portas de rede Gigabit 10/100/1000Mbps dual-switched, de deteção automática e PoE;
- Conferência de voz de 5 vias;
- Electronic Hook Switch (EHS);
- Até 6 contas SIP;
- Bluetooth USB e EHS (Electronic Hook-Switch) com possibilidade de mãos livres Plantronics ou outro;
- Possibilidade de autoatualizações usando TR-069 ou arquivo de configuração XML cifrado com AES, TLS/SRTP/HTTPS;
- Aplicações web integradas em tempo real;
- Módulo de expansão com informação visual sobre as teclas programadas.

- 2 (dois) Telefones avançados IP com TFT LCD a cores, com as seguintes características mínimas:

- 480x272 TFT LCD a cores com 4 linhas;
- LCD de 4.3”;
- 5 teclas programáveis sensíveis ao contexto;
- 24 teclas programáveis de extensão BLF;
- Dupla porta de rede Gigabit;
- PoE e Bluetooth integrados;
- Conferência de voz de 5 vias;
- Electronic Hook Switch (EHS);
- Até 6 contas SIP;
- Possibilidade de autoatualizações usando TR-069 ou arquivo de configuração XML cifrado com AES, TLS/SRTP/HTTPS;
- Aplicações web integradas em tempo real.

- 3 (três) Telefones IP DECT, com as seguintes características mínimas:

- Agenda com pelo menos 150 contactos;

- Som de alta definição;
- Ecrã colorido 4 linhas 1.8 " retro iluminado;
- Possibilidade de conectar um *headset* sem fios DECT;
- Teclado retro iluminado;
- Autonomia: pelo menos 20h em conversação / 220h em espera;
- Função mãos livres;
- Tempo de carga: max. 3h;
- Apresentação do nome e do número;
- Várias melodias e polifónicos;
- Função Bis (10 últimos números);
- Conferência a 3;
- Vários níveis de regulação de volume;
- Montagem mural possível;
- Plug & Play;
- Tecnologia ECO DECT.

- **61** (sessenta e um) **Telefones Base IP com LCD mono, com as seguintes características mínimas:**

- 2 portas de rede 10/100 Mbps;
- 1 conta SIP;
- 3 teclas programáveis;
- Visor LCD gráfico de 128x40 pixels;
- Conferência a 3;
- Agenda até 500 contactos;
- Histórico de chamadas 200 registos;
- Timbre personalizável;
- Função alta voz;
- Serviço de informações.

2. Caixas de correio eletrónico (e-mail)

O adjudicatário deverá fornecer um serviço de caixas de e-mail suportado em servidor mínimo Microsoft Exchange 2016 ou equivalente. A entidade adjudicante pretende adquirir caixas de e-mail de 2 tipos - caixas PRO e caixas Standard, nas seguintes quantidades:

- **10** (dez) caixas de e-mail PRO (60GB);
- **80** (oitenta) caixas de e-mail Standard (5GB).

A capacidade de total de espaço de alojamento (**1000GB**) **deverá ser partilhada da entre todas as caixas de e-mail**. A tabela seguinte resume as funcionalidades mínimas que cada tipo de caixa de e-mail deve possuir para utilização em computadores e *smartphones* da entidade adjudicante.

Funcionalidades	E-mail PRO		E-mail Standard	
	Computador	Smartphone	Computador	Smartphone
Capacidade mínima	60GB		5GB	
Acesso				
Via Web Access (WA)	x	x	x	x
Sincronização com cliente de e-mail	x	x	x	x
Calendário				
Consulta	x	x	Via WA	Via WA
Sincronização com cliente de e-mail	x	x	-	-
Visualização de disponibilidade (livre/ocupado)	x	x	Via WA	-
Gestão (aceitar, rejeitar, marcar reuniões)	x	x	Via WA	-
Contatos				
Partilha de contatos	x	x	Via WA	-
Lista de distribuição	x	x	x	x
Outras características				
Assistente out-of-office	x	x	Via WA	-
Criação de alias	x	x	x	x

Pastas partilhadas	x	x	Via WA	-
Tarefas partilhadas	x	x	Via WA	-
Anti-vírus	x	x	x	x
Anti-spam	x	x	x	x
IMAP4	x	x	x	x
ActiveSync	x	x	-	-
MAPI	x	x	-	-

3. Equipamentos e serviços de voz e internet para rede móvel

3.1. Serviço de comunicações GSM

O adjudicatário deverá ser **proprietário de uma infraestrutura com cobertura geográfica nacional** capaz de suportar as comunicações GSM da entidade adjudicante.

Através de **roaming**, o adjudicatário deve garantir que todo o tipo de comunicações **funcionará fora do território nacional**.

A entidade adjudicante pretende adquirir um **pacote de 30 cartões mantendo os atuais números** de telefone. Os mesmos serão apresentados mais adiante na separação por perfis.

O conjunto de 30 números móveis, juntamente com as 67 posições da rede fixa atrás descritas constituem a rede privada ou conta da entidade adjudicante. **Todas as SMS e chamadas efetuadas entre números da conta, deverão ser grátis e ilimitadas**. Para todos os cartões, a entidade adjudicante poderá solicitar gratuitamente um SIM gémeo.

Pretende-se a distribuição dos 30 cartões **por 5 perfis com caraterísticas distintas**, sendo que, **dentro de cada perfil, o número de minutos disponível por cartão deverá ser agrupado por forma a ficar partilhado entre todos os cartões de cada perfil**. O concorrente deverá indicar o preço de cada perfil por forma a calcular o **custo mensal fixo** a pagar.

Seguidamente, apresentam-se os números pertencentes aos perfis, bem como, as suas caraterísticas de ciclo mensal:

Perfil A (2 cartões) – Comunicações ilimitadas para própria rede e redes fixas nacionais; 2000 minutos/SMS para outras redes móveis e 10GB de tráfego internet.

- 962448242
- 932123500

Perfil B (2 cartões) – Comunicações ilimitadas para própria rede e redes fixas nacionais; 2000 minutos/SMS para outras redes móveis e 5GB de tráfego internet.

- 961742077
- 968425082

Perfil C (5 cartões) – Comunicações ilimitadas para própria rede e redes fixas nacionais; 2000 minutos/SMS para outras redes móveis e 500MB de tráfego internet.

- 963445817
- 961742057
- 968425081
- 962505874
- 961742050

Perfil D (6 cartões) – Com 250 minutos/SMS mensais para todas as redes nacionais e 500MB de tráfego internet.

- 963445928
- 968425085
- 963445829
- 968489060
- 963445877
- 963445866

Perfil E (15 cartões) – Com 100 minutos/SMS mensais para todas as redes nacionais e sem tráfego internet. A ligação internet deve ser bloqueada nestes cartões, pelo que, a entidade adjudicante não poderá ser responsabilizada pelo pagamento de tráfego internet em nenhum destes cartões.

- 964389569
- 962026255
- 963445818
- 964389501
- 962505873
- 961742053
- 963445938
- 967899927
- 968425083
- 962026296
- 966456958
- 966156432
- 968489065
- 963445880
- 963445814

Para as comunicações realizadas fora do que é contemplado em cada perfil, ou após esgotados os tráfegos previstos, o concorrente deverá apresentar os preços detalhadamente.

O preço de chamadas e SMS para redes fixas e móveis nacionais não deve ultrapassar os 0,04€ por minuto/SMS.

Devem ser apresentados os **preços por minuto** para **comunicações internacionais/roaming**, e estes devem estar enquadradas com os valores de referência do mercado. O concorrente deverá também apresentar estes preços detalhadamente.

Não será necessário apresentar o preço de MMS, uma vez que estas, bem como a subscrição de conteúdos digitais deve estar desativada em todos os cartões.

O concorrente deve apresentar preços de outros serviços não contemplados no presente Caderno de Encargos.

3.2. Equipamentos terminais móveis de comunicação

Para realizar as comunicações descritas no número anterior, o adjudicatário deverá **ceder gratuitamente à entidade adjudicante equipamentos comunicação**.

Esta cedência divide-se em 2 fases. A primeira fase contempla a operacionalização inicial dos serviços. Nesta fase o adjudicatário deverá ceder para utilização da entidade adjudicante os seguintes equipamentos ou equivalentes:

- 2 (dois) Smartphones equivalentes ou superior a iPhone 11 128GB preto mate;
- 1 (um) Smartphone equivalente ou superior a iPhone 7 32GB preto mate;
- 10 (dez) Smartphones equivalentes ou superior a Huawei P30 Lite DS;
- 17 (dezassete) telemóveis 2G.

A segunda fase decorre durante os 24 meses do período de vigência do contrato e inclui a possibilidade de a entidade adjudicante receber mais equipamentos por forma a modernizar ou substituir os da fase anterior.

Para este efeito, o adjudicatário deverá disponibilizar um *plafond* para equipamentos que deverá ser **igual ou superior a 2.500,00€ (+IVA)**, devendo o concorrente apresentar **uma tabela de preços com equipamentos** atuais de diversas gamas para que a entidade adjudicante possa escolher os que pretender até atingir o valor do *plafond*.

3.3. Banda Larga móvel

A entidade adjudicante também pretende adquirir **serviços de conectividade internet em banda larga móvel** nas quantidades apresentadas na tabela seguinte. Para estes serviços o concorrente deverá apresentar os preços de acordo com a tabela e deverá também referir as larguras de banda garantidas nas comunicações.

Quantidade	Volume de tráfego mensal	Mensalidade	Plafond extra (Preço/MB)
1	7GB	<= 7,50€	
2	75GB	<= 15,00€	

Nestes cartões, a entidade adjudicante vai solicitar **gratuitamente cartões SIM gémeos**.

4. Servidores virtuais privados, serviços, comunicações e equipamento

A entidade adjudicante pretende adquirir serviços de Data Center *Virtual (DCV)* onde o seja possível a criação e administração de Virtual Machines (VM) utilizando recursos computacionais disponibilizados pelo adjudicatário.

Estes serviços deverão ser suportados num Data Center (DC) proprietário do adjudicatário e estar integrados numa plataforma do tipo portal *self-service* por forma permitir a provisão automática e flexível de recursos por parte da entidade adjudicante.

Os serviços de *DCV* serão utilizados pela entidade adjudicante nas suas instalações em Vila Velha de Ródão, neste sentido, as comunicações até ao DC do adjudicatário, bem como segurança das mesmas, devem ser contempladas no presente procedimento.

4.1. Caraterísticas do Data Center do adjudicatário

O Data Center do adjudicatário deve localizar-se em **território nacional** e possuir as seguintes **certificações** mínimas comprovadas:

- Certificação Tier III (pelo Uptime Institute) em termos de conceção e instalação, que implica a garantia que todo o projeto de infraestrutura segue um princípio de redundância N+1, por forma a alcançar uma disponibilidade anual mínima de 99,98%;
- Sistema de Gestão da Tecnologia da Informação conforme os requisitos da ISO/IEC 20000-1 para Data Center e Cloud Services;
- Sistema de Gestão da Segurança da Informação conforme aos requisitos da ISO/IEC 27001 para os serviços de TI relativos a Data Center e Cloud;
- Sistemas de deteção e extinção de incêndios conforme os requisitos da ISO 14520;
- Sistemas de gestão da qualidade conforme os requisitos da ISO 9001.

Como **complemento** às certificações do Data Center, deverá estar assegurado um conjunto de **procedimentos e requisitos**, descritos de seguida:

- Dispor de um centro dedicado que assegure toda a operação e supervisão das instalações numa base permanente (24x7x365);
- O edifício de implantação deverá contar com a presença permanente de uma equipa de segurança de modo a garantir um rigoroso controlo de acessos. Internamente, devem existir vários perímetros e a movimentação dentro de cada um deles ser restrita e controlada através de alarmística e circuitos CCTV;
- Ser garantida redundância de sistemas ao nível do fornecimento de energia elétrica. Em caso de falha, todos os sistemas deverão dispor de equipamentos redundantes, tais como UPS, Baterias e Geradores.

4.2. Plataforma de gestão

Para **gestão dos recursos** contratados e administração dos sistemas, deverá existir uma **plataforma de gestão online** com as seguintes caraterísticas mínimas:

- Uma interface de gestão *web* simples e intuitiva para permitir a disponibilização ágil e em tempo real de recursos lógicos computacionais com elevada segurança, escalabilidade e disponibilidade;
- Suportar a implementação de diferentes sistemas operativos e aplicações através de um ambiente virtual dedicado, constituído por recursos de processamento, de memória, de armazenamento e de rede totalmente flexíveis;
- Permitir a virtualização de contextos de *firewall*, isolamento de rede, possibilidade de definição de políticas de segurança entre aplicações ou VM para permitir ou bloquear comunicação na mesma rede local virtual ou em redes locais virtuais distintas;
- Deverá estar alojada em ambiente protegido e com redundância implementada, por forma a estar sempre acessível;
- Deverá permitir a implementação e regras para distribuição tráfego entre VM ou para implementar mecanismos de *failover*;
- Deverá permitir a realização de cópias de segurança das VM, possibilitando a definição da frequência e o período de retenção, viabilizando também a possibilidade de recuperação da informação através de restauro de qualquer cópia de segurança realizada;
- Permitir a monitorização remota do estado das VM e dos seus recursos, por forma a ajustar a capacidade proactivamente;
- Deverá permitir a transferência de VPS de outras infraestruturas, virtualizadas ou não, para a plataforma virtual e vice-versa, recorrendo a formatos de VM compatíveis;
- Deverá disponibilizar ferramentas (API) que permitam a gestão de servidores sem intervenção manual;
- Possuir um sistema de *backup* centralizado e, se necessário, futuramente, um serviço de *disaster recovery*, suportado em DC secundário ligado ao principal por VPN.

4.3. Software disponível

Para facilitar a implementação de serviços e configuração de VM's, a plataforma de gestão deverá possuir um **catálogo de sistemas operativos com *templates* passíveis de serem utilizados**.

Deverá existir um **conjunto alargado de imagens**, que compreendam os **mais recentes** sistemas operativos **Microsoft e Linux**.

4.4. Segurança, conectividade e comunicações

Para além da exigência do Data Center obedecer a todas as garantias de segurança, a **conectividade e comunicações até às instalações da entidade adjudicante deverão também garantir elevados padrões de segurança**.

Para garantir o controlo de acesso à informação, deverão ser contempladas e apresentadas medidas de segurança, fazendo uso de mecanismos tais como: VPN; IDS; IPS e Firewall. Deverá igualmente ser apresentado o tipo de encriptação da VPN.

Complementarmente a estes mecanismos, o adjudicatário deverá disponibilizar uma equipa de SOC (Security Operations Centre) com o objetivo de identificar e correlacionar eventos de acesso a sistemas em tempo real.

A gestão da segurança do adjudicatário deve disponibilizar com regularidade, ou sempre que solicitado, informação relativa aos aspetos de segurança da infraestruturas e serviços, contemplando relatórios tipo:

- Relatórios das principais vulnerabilidades apresentadas no período em questão;
- Planos de ação, para colmatar potenciais vulnerabilidades identificadas;
- Relatórios de questões de segurança identificadas e resolvidos;

- Propostas de melhoria da política de segurança em prática;
- Identificação e caracterização das condições em cada violação de segurança que tenha ocorrido no período.

No presente procedimento, pretende-se adquirir **acesso apenas ao back-end do DCV** não existindo, portanto, necessidade de ligação entre o DCV e a Internet. Deverá ser providenciada uma **ligação VPN num circuito com largura de banda de 200/200Mbps**, sendo este suportado na ligação fibra ótica Gigabit Ethernet do ponto 1.1. da parte II deste Caderno de Encargos. O **tráfego** deverá ser **ilimitado**.

Os componentes do **DCV** bem como a **ligação** até às instalações da entidade adjudicante, deverão **ser passíveis de configuração por forma a se apresentarem como transparentes para a restante infraestrutura da entidade adjudicante**, fazendo, neste caso, **utilização do mesmo endereçamento IPv4: 172.17.0.0/16**.

4.5. Prestação dos serviços

O adjudicatário deverá garantir **disponibilidade mínima de serviço do DCV de 99,95%** e também suporte técnico especializado 24 x 7 x 365, bem como suporte telefónico comercial 7x5.

Para comprovar o nível de serviço, o concorrente **deverá apresentar detalhadamente o SLA** (acordo de nível de serviço) proposto, sendo que o mesmo se deve enquadrar nos valores de referência do mercado.

4.6. Recursos computacionais requeridos

Para implementação de VM's no DCV a adquirir no presente procedimento, a entidade adjudicante requer os seguintes **recursos computacionais**:

- **6** (seis) Módulos de computação com 1vCPU + 2GB vRAM;
- **4** (quatro) Módulos de armazenamento base SSD com 100GB;
- **5** (cinco) Módulos de armazenamento base SATA com 1TB.

O concorrente deverá referir todas as especificações técnicas relativamente aos recursos computacionais apresentados. Os vCPU respeitantes aos módulos de computação deverão ter por base equivalente ou superior a Intel Xeon 2,66 Ghz; A ligação entre VM's no DCV deverá ser de 10Gbps ou superior; Por cada VM deverá ser possível associar 4,5TB de armazenamento ou mais.

As quantidades apresentadas constituem o **máximo que a entidade adjudicante poderá utilizar** ao abrigo do presente procedimento, no entanto, **não se vincula ao uso da totalidade dos recursos contratados**, comprometendo-se a provisionar, no mínimo, um quarto dos recursos requeridos no presente procedimento.

Para facilitar a elaboração da proposta e a sua análise, o concorrente deverá apresentar a seguinte tabela preenchida nos campos em branco com os preços propostos. Para o efeito, deve utilizar o ficheiro XLSX que acompanha os documentos do procedimento.

CMVVR - Aquisição de serviços de comunicações, VPS e aluguer de equipamentos

	Pr. Unitário	Quantidade	Preço Total
Dados, voz fixa e central telefónica virtual			
Ligação fibra ótica Gigabit Ethernet - 1000BaseT		1	- €
Conetividade 300/300Mbps, tráfego ilimitado		1	- €
Conetividade VoIP 16 canais		1	- €
Utilizadores central telefónica virtual		67	- €
Flat rate dos 16 canais VoIP		16	- €
Fax Online		1	- €
Número verde		1	- €
Plataforma de envio de SMS 3000/mês			
		1	- €
Aluguer de equipamentos			
Telefone Base		61	- €
Módulo Teclas Extra		4	- €
Telefone Avançado		3	- €
Telefone IP DECT		3	- €
Router CPE		1	- €
Outros serviços e ligações fibra ótica/ADSL			
FO internet 1000/200Mbps, tráfego ilimitado + voz		1	- €
FO internet 1000/200Mbps, tráfego ilimitado + voz + TV		2	- €
FO internet 100/100Mbps, tráf. ilimitado + voz + TV		1	- €
ADSL internet 16/1Mbps, tráfego ilimitado + voz + TV		1	- €
Linha analógica 500+100 min. sem equipamento			
		6	- €
Total de redes fixas, ligações/conetividade internet e SMS:			- €
Caixas de e-mail com capacidade partilhada			
Caixa de correio eletrónico PRO (60GB)		10	- €
Caixa de correio eletrónico Standard (5GB)		80	- €
Total de caixas de e-mail			- €
Equipamentos e serviços de voz e dados para rede móvel			
Cartões móveis Perfil A (ilim. pr. rede, 2000 min/SMS, 5GB net)		2	- €
Cartões móveis Perfil B (250 min/SMS, 5GB net)		2	- €
Cartões móveis Perfil C (250 min/SMS, 500MB net)		6	- €
Cartões móveis Perfil D (ilim. pr. rede, 2000 min/SMS, 500MB net)		5	- €
Cartões móveis Perfil E (100 min/SMS, SEM net)		15	- €
Banda larga móvel 75GB/mês		2	- €
Banda larga móvel 7GB/mês		1	- €
Plafond para equipamentos 2ª fase	>= 2500,0€		
Total de equipamentos e serviços de voz e internet para rede móvel:			- €
Servidores virtuais privados (VPS), serviços, comunicações e equipamento			
VPS - Módulo de computação com 1vCPU + 2GB vRAM		6	- €
VPS - Armazenamento base SSD com 100GB		4	- €
VPS - Armazenamento base SATA com 1TB		5	- €
Conectividade VPN e back-end 200/200Mbps, tráfego ilimitado		1	- €
Total de VPS, serviços, comunicações e equipamento:			- €
Resumo			
Custos fixos mensais		- €	
Custos variáveis mensais		400,00 €	
Total mensal		400,00 €	
Total do contrato (24 meses)		9.600,00 €	

Anexo RGD

ÍNDICE

Introdução	3
Clausulado-Tipo Contratual	4
1. Preâmbulo	5
2. Os direitos e obrigações do responsável pelo tratamento	6
3. O subcontratante atua de acordo com instruções	6
4. Confidencialidade	7
5. Segurança do tratamento	7
6. Recurso a subsubcontratantes	9
7. Transferências de dados pessoais para países terceiros ou organizações internacionais	10
8. Assistência ao responsável pelo tratamento	11
9. Notificação de uma violação de dados pessoais	13
10. Apagamento e devolução de dados	14
11. Auditoria e inspeção	15
12. Acordo entre as partes relativamente a outros termos	15
13. Início e término	15
14. Pontos de contacto do responsável pelo tratamento e do subcontratante	17
Anexo A: Informação sobre o Tratamento	18
A.1. A finalidade do tratamento realizado pelo subcontratante em nome do responsável pelo tratamento é:	18

A.2. O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento deverá maioritariamente limitar-se a (natureza do tratamento):.....	18
A.3. O tratamento inclui os seguintes tipos de dados pessoais relativamente aos titulares dos dados:.....	19
A.4. O tratamento inclui as seguintes categorias de titulares dos dados:.....	19
A.5. O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento poderá ser realizado quando as cláusulas tenham início. O tratamento tem a seguinte duração:	19
Anexo B: Instrução relativa ao tratamento de dados pessoais.....	21
B.1. Objeto de instrução de tratamento.....	21
B.2. Segurança do tratamento	21
Requisitos técnicos mínimos das redes e sistemas de informação (conforme a Resolução de Ministros n.º 41/2018).....	23
B.3. Prestação de assistência ao responsável pelo tratamento.....	44
B.4. Período de armazenamento/procedimentos de apagamento.....	44
B.5. Localização do tratamento	45
B.6. Instrução para a transferência de dados pessoais para países terceiros.....	45
B.7. Procedimentos para a realização de auditorias pelo responsável pelo tratamento, incluindo inspeções, do tratamento de dados pessoais realizados pelo subcontratante em nome do responsável pelo tratamento	45

INTRODUÇÃO

No contexto europeu e nacional têm vindo a ser criados/reforçados mecanismos de salvaguarda dos indivíduos, no que à proteção de dados diz respeito.

Desde logo, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados - RGPD) traz consigo novas obrigações para os responsáveis pelo tratamento de dados e novos e reforçados direitos para os titulares.

No contexto nacional, a Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD, tem também disposições específicas no que ao tratamento de dados diz respeito.

Finalmente, a Resolução do Conselho de Ministros n.º 41/2018, contém requisitos técnicos mínimos aplicáveis à Administração direta e indireta do Estado, servindo como modelo para o setor privado.

O Município de Vila Velha de Ródão tem como objetivo assegurar o cumprimento de todas as disposições legais que lhe são aplicáveis no contexto da proteção de dados.

Neste sentido, o presente documento oferece as cláusulas-tipo de proteção de dados, conforme adotadas pela Autoridade de Controlo Dinamarquesa e revistas pelo Comité Europeu de Proteção de Dados, com acrescento das disposições constantes na Resolução do Conselho de Ministros n.º 41/2018, relativas aos requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado, servindo também como um modelo para o setor empresarial do Estado e para o setor privado.

CLAUSULADO-TIPO CONTRATUAL

Para os fins definidos no Artigo 28, n.º 3 do Regulamento 2016/679 (RGPD)

entre

Município de Vila Velha de Ródão

NIPC 506642798

Rua Santana,

6030-230 Vila Velha de Rodão

(o responsável pelo tratamento)

e

o adjudicatário

(o subcontratante)

Designadas como “parte”; no seu conjunto como “as partes”

CONCORDAM nas seguintes cláusulas contratuais (as cláusulas) de modo a cumprir os requisitos do RGPD e assegurar a proteção dos direitos do titular de dados.

1. Preâmbulo

1. Estas cláusulas contratuais (as cláusulas) estipulam os direitos e obrigações do responsável pelo tratamento bem como do subcontratante, quando este trata dados pessoais em nome do responsável pelo tratamento.
2. As cláusulas foram desenhadas para assegurar a conformidade das partes relativamente ao Art.28º, n.º 3 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados - RGPD).
3. No contexto do fornecimento dos serviços de comunicações, servidores virtuais e aluguer de equipamentos e fornecimento de serviços de e-mail, o subcontratante irá processar dados pessoais em nome do responsável pelo tratamento, de acordo com as cláusulas.
4. As cláusulas devem ser prioritárias face a quaisquer outras disposições contidas em acordos entre as partes.
5. Dois Anexos são adicionados às cláusulas e são parte integrante das mesmas.
6. O Anexo A contém detalhes relativamente ao tratamento de dados pessoais, incluindo as finalidades e a natureza do tratamento, tipo de dados pessoais, categorias de titulares de dados e duração do tratamento.
7. O Anexo B contém as instruções do responsável pelo tratamento relativamente ao tratamento de dados pessoais, as medidas de segurança mínimas que devem ser implementadas pelo subcontratante e como as auditorias do subcontratante e de outros subcontratantes ulteriores devem ser realizadas.
8. As cláusulas, bem como os anexos, devem ser mantidos na forma escrita, incluindo a forma eletrónica, pelas partes.

9. As cláusulas não isentam o subcontratante de obrigações a que este esteja sujeito relativamente ao RGPD ou outra legislação.

2. Os direitos e obrigações do responsável pelo tratamento

1. O responsável pelo tratamento é responsável por assegurar que o tratamento de dados pessoais se encontra em conformidade com o RGPD (ver Art.24º do RGPD), com as disposições de proteção de dados europeias ou dos Estados-Membros que lhe sejam aplicáveis e com as cláusulas.

2. O responsável pelo tratamento tem o direito e a obrigação de tomar decisões sobre as finalidades e os meios do tratamento de dados pessoais.

3. O responsável pelo tratamento deverá ser responsável, entre outros, por assegurar que o tratamento de dados pessoais que é realizado pelo subcontratante em seu nome, através de instruções definidas por si, tem um fundamento legal.

3. O subcontratante atua de acordo com instruções

1. O subcontratante deve tratar dados pessoais apenas mediante instruções documentadas fornecidas pelo responsável pelo tratamento, a menos que tal seja requerido pela legislação aplicável ao subcontratante. Tais instruções devem ser especificadas no Anexo A e B. Instruções posteriores podem ser fornecidas pelo responsável pelo tratamento durante o tratamento de dados pessoais, mas tais instruções deverão sempre ser documentadas e mantidas na forma escrita, incluindo o formato eletrónico, em relação com as cláusulas.

2. O subcontratante deverá imediatamente informar o responsável pelo tratamento se instruções fornecidas pelo responsável pelo tratamento, na opinião do subcontratante, contrariando o RGPD ou outra disposição legal aplicável relativa à proteção de dados.

3. No caso de se verificar a emissão de instruções potencialmente desconformes fornecidas pelo responsável pelo tratamento, sendo estas identificadas pelo

subcontratante, este deve proceder a uma comunicação relativamente a este facto ao responsável pelo tratamento, para que este possa proceder à sua retificação. Caso este facto não seja identificado pelo subcontratante ou pelo responsável pelo tratamento, mas sim por terceiros, as mesmas serão consideradas inválidas no momento da sua identificação, tendo efeitos retroativos. As partes deverão acordar entre si quais serão as ações necessárias a tomar, atendendo à situação contextual.

4. Confidencialidade

7

1. O subcontratante deverá conceder acesso a dados pessoais tratados em nome do responsável pelo tratamento a pessoas que estejam sob a autoridade do subcontratante que se tenham comprometido a assegurar a confidencialidade ou estejam sob estatutos apropriados que garantam o dever de sigilo e confidencialidade, seguindo o princípio da necessidade de conhecer. A lista de pessoas a quem o acesso foi concedido deverá ser alvo de revisão periódica. Nesta revisão, o acesso a dados pessoais pode ser removido, se tal acesso não for mais necessário, sendo que tais dados pessoais consequentemente não deverão ser mais acessíveis a tais pessoas.

2. O subcontratante deverá, a pedido do responsável pelo tratamento, demonstrar que as pessoas sob sua autoridade estão sujeitas à obrigação de confidencialidade e sigilo.

5. Segurança do tratamento

1. O Art.32º do RGPD estipula que, considerando o estado da arte, os custos da implementação e a natureza, âmbito, contexto e finalidades do tratamento, bem como o risco de probabilidade e gravidade variável para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante deverão implementar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança apropriado ao risco.

O responsável pelo tratamento deverá avaliar os riscos para os direitos e liberdades das pessoas singulares inerentes ao tratamento e implementar medidas para mitigar tais riscos.

Dependendo da sua relevância, as medidas podem incluir:

- a. Pseudonimização e cifragem dos dados pessoais;
 - b. A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
 - c. A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
 - d. Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.
2. De acordo com o Art.32º do RGPD, o subcontratante deverá também – independentemente do responsável pelo tratamento – avaliar os riscos para os direitos e as liberdades das pessoas singulares inerentes ao tratamento e implementar medidas para mitigar tais riscos. Para este efeito, o responsável pelo tratamento deverá fornecer ao subcontratante toda a informação necessária para identificar e avaliar tais riscos.
3. O subcontratante deverá auxiliar o responsável pelo tratamento a garantir a conformidade com as obrigações do responsável pelo tratamento no que ao Art.32º do RGPD diz respeito por, nomeadamente, fornecer ao responsável pelo tratamento informação relativa a medidas técnicas e organizativas já implementadas pelo subcontratante no cumprimento deste mesmo artigo, bem como outra informação necessária para que o responsável pelo tratamento esteja em conformidade com as suas obrigações no cumprimento do já citado Art.32º do RGPD.

Se subseqüentemente – na avaliação realizada pelo responsável pelo tratamento – a mitigação dos riscos identificados requerer medidas adicionais a serem aplicadas pelo

subcontratante, além das que já foram implementadas pelo mesmo no cumprimento do Art.32º do RGPD, o responsável pelo tratamento deverá especificar tais medidas adicionais a serem implementadas no Anexo B.

6. Recurso a subsubcontratantes

1. O subcontratante deverá cumprir os requisitos especificados no Art.28º, n.º 2 e n.º 4 do RGPD quando contratar outro subcontratante (um subsubcontratante).
2. O subcontratante não deverá, portanto, contratar outro subcontratante (um subsubcontratante) para o cumprimento das cláusulas sem a prévia autorização geral escrita do responsável pelo tratamento.
3. O subcontratante tem uma autorização geral escrita para contratar subsubcontratantes. O subcontratante deverá informar, por escrito, o responsável pelo tratamento de quaisquer mudanças relativamente quanto ao aumento do número ou à substituição de outros subcontratantes pelo menos com a antecedência de 30 dias, fornecendo assim ao responsável pelo tratamento a possibilidade de se opor a tais alterações antes de os subsubcontratantes serem contratados.
4. Quando o subcontratante contratar um subsubcontratante para realizar um atividades de tratamento de dados específicas em nome do responsável pelo tratamento, as mesmas obrigações relativas à proteção de dados, conforme definidas nas cláusulas, devem ser impostas a esse mesmo subsubcontratante, sob a forma de um contrato ou outro ato legal conforme o direito europeu ou lei de Estado-Membro, em particular fornecendo garantias suficientes para implementar medidas técnicas e organizativas adequadas, de um modo que o tratamento cumpra os requisitos das cláusulas e do RGPD.

O subcontratante deverá, portanto, ser responsável para requerer que esse subsubcontratante pelo menos cumpra com as obrigações às quais o subcontratante se encontra sujeito relativamente às cláusulas e ao RGPD.

5. Uma cópia de tal acordo com o subsubcontratante e as subseqüentes adendas deverá – face a um pedido do responsável pelo tratamento – ser submetido ao responsável pelo tratamento, oferecendo-lhe assim a oportunidade de assegurar que as mesmas obrigações no contexto da proteção de dados definidas nas cláusulas são impostas ao subsubcontratante. Cláusulas relacionadas com questões de negócio que não afetem o conteúdo legal relativo a proteção de dados do acordo com o subsubcontratante não são submetidas para envio ao responsável pelo tratamento.

6. O subcontratante deverá realizar um contrato a favor de terceiro com o subsubcontratante onde – no caso da falência do subcontratante – o responsável pelo tratamento deverá ser a parte beneficiária do contrato com o subsubcontratante e deverá ter o direito a fazer cumprir o contrato com o subsubcontratante em que o subcontratante era parte, por exemplo, permitindo ao responsável pelo tratamento a instruir o subsubcontratante a eliminar ou devolver dados pessoais que eram objeto do contrato referido.

7. Caso o subsubcontratante não cumpra as suas obrigações no contexto da proteção de dados, o subcontratante deverá ser plenamente responsável face ao responsável pelo tratamento no que diz respeito ao cumprimento das obrigações do subsubcontratante. Isto não afeta os direitos dos titulares de dados no que ao RGPD diz respeito - em particular os que se encontram previstos nos Artigos 79.º e 82.º do RGPD – face ao responsável pelo tratamento e subcontratante, incluindo o subsubcontratante.

7. Transferências de dados pessoais para países terceiros ou organizações internacionais

1. Qualquer transferência de dados pessoais para países terceiros ou organizações internacionais pelo subcontratante deverão apenas ocorrer tendo por base instruções documentadas do responsável pelo tratamento e deverão sempre ser realizadas em conformidade com o Capítulo V do RGPD.

2. No caso de transferências para países terceiros ou organizações internacionais, realizadas pelo subcontratante sem instruções documentadas por parte do responsável pelo tratamento, que são requeridas pelo direito da União ou de Estado-Membro a que o subcontratante se encontre sujeito, o subcontratante deverá informar o responsável pelo tratamento dessa obrigação jurídica antes de iniciar o tratamento, a menos que essa lei proíba tal informação tendo por base motivos de interesse público.

3. Sem instruções documentadas por parte do responsável pelo tratamento, o subcontratante não pode, no âmbito das cláusulas:

- a. transferir dados pessoais para outro responsável pelo tratamento ou para um subcontratante num país terceiro ou numa organização internacional;
- b. transferir o tratamento de dados pessoais para um subsubcontratante num país terceiro;
- c. ter dados pessoais tratados por si num país terceiro.

4. As instruções do responsável pelo tratamento relativas à transferência de dados pessoais para um país terceiro incluindo, se aplicável, o mecanismo de transferência previsto no Capítulo V do RGPD no qual são baseadas, deverão ser definidas no Anexo B.6.

5. As cláusulas não devem ser confundidas com cláusulas standard de proteção de dados conforme o significado do Art.46º, n.º 2, al. c) e d) do RGPD e as cláusulas não podem ser encaradas pelas partes como um mecanismo de transferência previsto no Capítulo V do RGPD.

8. Assistência ao responsável pelo tratamento

1. Considerando a natureza do tratamento, o subcontratante deverá auxiliar o responsável pelo tratamento por medidas técnicas e organizativas adequadas, na medida do possível. No cumprimento das obrigações do responsável pelo tratamento para responder aos

pedidos relativos ao exercício de direitos dos titulares de dados descritos no Capítulo III do RGPD.

Isto implica que o subcontratante deverá, na medida do possível, prestar assistência ao responsável pelo tratamento na conformidade com:

- a. o direito a ser informado quando haja recolha de dados pessoais do titular dos dados;
- b. o direito a ser informado quando dados pessoais não tenham sido recolhidos junto do titular dos dados;
- c. o direito do acesso do titular de dados;
- d. o direito de retificação;
- e. o direito ao apagamento dos dados ("direito a ser esquecido");
- f. o direito à limitação do tratamento;
- g. a obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento;
- h. o direito de portabilidade dos dados;
- i. o direito de oposição;
- j. o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis.

2. O subcontratante deverá, considerando a natureza do tratamento e a informação disponível para o subcontratante, prestar assistência ao responsável pelo tratamento, de modo a assegurar conformidade com:

- a. A obrigação do responsável pelo tratamento para, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, notificar a violação de dados pessoais à autoridade de controlo competente, nomeadamente

a Comissão Nacional de Proteção de Dados (CNPD), a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

b. A obrigação do responsável pelo tratamento para, sem demora injustificada, comunicar a violação de dados pessoais ao titular dos dados, quando esta for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares;

c. A obrigação do responsável pelo tratamento de realizar uma Avaliação de Impacto sobre a Proteção de Dados relativamente a um determinado tratamento;

d. A obrigação do responsável pelo tratamento de consultar a autoridade de controlo competente, nomeadamente a CNPD, antes de iniciar o tratamento quando uma Avaliação de Impacto sobre a Proteção de Dados indicar que o tratamento resultaria num risco elevado na ausência de medidas implementadas pelo responsável pelo tratamento para mitigar o risco.

3. As partes deverão definir no Anexo B as medidas técnicas e organizativas adequadas pelas quais o subcontratante é requerido a prestar assistência ao responsável pelo tratamento, bem com o âmbito e extensão da assistência requerida. Tal aplica-se a todas as obrigações previstas nas cláusulas 8.1. e 8.2.

9. Notificação de uma violação de dados pessoais

1. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais.

2. A notificação do subcontratante ao responsável pelo tratamento deverá ser realizada até 48 horas depois de o subcontratante ter tomado conhecimento da violação de dados pessoais, de modo a permitir ao responsável pelo tratamento cumprir com a sua

obrigação de notificar a violação de dados pessoais à autoridade de controlo competente, conforme o Art.33º do RGPD.

3. De acordo com a cláusula 8.2, al. a), o subcontratante deverá prestar assistência ao responsável pelo tratamento na notificação da violação de dados à autoridade de controlo competente, significando tal que o subcontratante deverá prestar assistência na obtenção de informação listada abaixo, a qual, em conformidade com o Art.33, n.º 3 do RGPD, deverá constar na notificação submetida à autoridade de controlo competente:

- a. A natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
- b. As consequências prováveis da violação de dados pessoais;
- c. As medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

10. Apagamento e devolução de dados

1. Depois de concluída a prestação de serviços relacionados com o tratamento de dados pessoais, o subcontratante é obrigado a devolver todos os dados pessoais ao responsável pelo tratamento e a eliminar as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros.

2. Caso o direito da União ou dos Estados-Membros aplicável ao subcontratante requeira o armazenamento de dados pessoais depois do término da prestação de serviços de tratamento de dados pessoais, este poderá manter esta informação apenas para as finalidades determinadas na lei.

O subcontratante compromete-se a tratar exclusivamente os dados pessoais para as finalidades e duração indicadas pelas disposições legais suprarreferidas e estritamente considerando as condições aplicáveis.

11. Auditoria e inspeção

1. O subcontratante deverá disponibilizar ao responsável pelo tratamento toda a informação necessária para demonstrar conformidade com as obrigações dispostas no Art.28º do RGPD, bem como com as cláusulas, e permitir e contribuir para as auditorias, incluindo inspeções, conduzidas pelo responsável pelo tratamento ou outro auditor por si mandatado.
2. Os procedimentos aplicáveis para as auditorias do responsável pelo tratamento, incluindo inspeções, do subcontratante e dos subsubcontratantes são especificadas nos Anexos B.7. e B.8.
3. O subcontratante deverá ser requerido a fornecer às autoridades de controlo, que no cumprimento da legislação aplicável têm acesso às instalações do responsável pelo tratamento e do subcontratante, ou a representantes que atuam em nome da autoridade de controlo, acesso às instalações físicas do subcontratante mediante a apresentação de identificação adequada.

12.Acordo entre as partes relativamente a outros termos

1. As partes podem acordar outras cláusulas relativamente ao tratamento de dados pessoais especificando, por exemplo, responsabilidade, desde que estas não contrariem direta ou indiretamente as cláusulas ou prejudicam os direitos ou liberdades fundamentais do titular de dados e a proteção oferecida pelo RGPD.

13. Início e término

1. As cláusulas entram em vigor na data de assinatura das partes.

2. As partes podem requerer que as cláusulas sejam renegociadas se alterações a disposições legais ou a inadequação das cláusulas der azo a renegociação.

3. As cláusulas deverão ser aplicadas durante o período de tratamento de dados pessoais. Durante o período de tratamento de dados pessoais, as cláusulas não podem ser cessadas a menos que outras cláusulas tenham sido acordadas entre as partes relativamente à governação do tratamento de dados pessoais.

4. Se a prestação de serviços relativamente ao tratamento de dados pessoais cessar e os dados pessoais forem eliminados ou devolvidos ao responsável pelo tratamento conforme a cláusula 10.1 e o Anexo B.4., as cláusulas podem ser cessadas mediante aviso escrito por cada uma das partes.

5. Assinatura

Da parte do responsável pelo tratamento

Nome [NOME]

Posição [POSIÇÃO]

Data [DATA]

Assinatura [ASSINATURA]

Da parte do subcontratante

Nome [NOME]

Posição [POSIÇÃO]

Data [DATA]

Assinatura [ASSINATURA]

14. Pontos de contacto do responsável pelo tratamento e do subcontratante

1. As partes podem entrar em contacto utilizando os pontos de contacto abaixo discriminados.
2. As partes deverão ser obrigadas a informar continuamente a outra de alterações aos pontos de contacto existentes.

Responsável pelo tratamento

Nome [NOME]

Posição [POSIÇÃO]

Telefone [TELEFONE]

E-mail [E-MAIL]

Subcontratante

Nome [NOME]

Posição [POSIÇÃO]

Telefone [TELEFONE]

E-mail [E-MAIL]

ANEXO A: INFORMAÇÃO SOBRE O TRATAMENTO

A.1. A finalidade do tratamento realizado pelo subcontratante em nome do responsável pelo tratamento é:

O subcontratante realiza a prestação de serviços de comunicações, servidores virtuais e aluguer de equipamentos, bem como o fornecimento de serviços de caixas de e-mail.

A.2. O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento deverá maioritariamente limitar-se a (natureza do tratamento):

Relativamente à prestação de serviços de comunicações, são considerados os seguintes artigos:

- As chamadas telefónicas efetuadas e recebidas através da rede fixa;
- As chamadas telefónicas efetuadas e recebidas através da rede móvel;
- As SMS enviadas e recebidas através da plataforma *web* de envio e através da rede móvel;
- As ligações à internet estabelecidas através de redes fixas e através de banda larga móvel.

No âmbito da prestação de serviços de comunicações, poderão ser tratados dados relativos a comunicações, nomeadamente, o conteúdo das chamadas bem como os números de telefone atribuídos e metadados associados.

Relativamente aos servidores virtuais, estes serão utilizados essencialmente para serviços de backup de informação pertencente ao responsável pelo tratamento, podendo também ser utilizados para outros fins, caso assim seja necessário.

No que diz respeito ao tratamento de dados no âmbito do fornecimento de serviços de caixas de e-mail, o subcontratante disponibilizará caixas de e-mail, incluindo todos os

serviços que assegurem a continuidade e disponibilidade do mesmo durante o período de vigência do contrato.

A.3. O tratamento inclui os seguintes tipos de dados pessoais relativamente aos titulares dos dados:

Para efeitos da prestação de serviços de comunicações, serão tratados pelo subcontratante o conteúdo das comunicações, bem como metadados associados.

Para efeitos de utilização dos servidores virtuais, os mesmos poderão incluir os seguintes dados pessoais: nome, n.º de cartão de cidadão/Bi/passaporte, morada, NIF, contacto telefónico, endereço de e-mail, bem como todos os restantes dados associados a serviços prestados pelo responsável pelo tratamento. Relativamente a categorias especiais de dados, conforme o disposto no Art.9º do RGPD, poderão ser tratados dados de saúde, dados relativos a filiação sindical, bem como dados relativos à esfera íntima e particular do titular dos dados, relativamente à sua situação socioeconómica, familiar, dados que caracterizam a situação de vulnerabilidade social do titular, entre outros.

No âmbito da prestação de serviços de caixas de e-mail, poderão ser alvo de tratamento os seguintes dados pessoais: nome, endereço de e-mail, assinatura eletrónica, telefone, bem como dados pessoais incluídos no conteúdo das mensagens de e-mail.

A.4. O tratamento inclui as seguintes categorias de titulares dos dados:

O tratamento inclui as seguintes categorias de titulares de dados: trabalhadores, munícipes, terceiros que interajam com o responsável pelo tratamento.

A.5. O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento poderá

ser realizado quando as cláusulas tenham início. O tratamento tem a seguinte duração:

O tratamento a ser realizado pelo subcontratante terá a duração máxima de 24 meses, com exceção do período necessário por imposições legais ao subcontratante.

ANEXO B: INSTRUÇÃO RELATIVA AO TRATAMENTO DE DADOS PESSOAIS

B.1. Objeto de instrução de tratamento

O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento deverá ser realizado pelo subcontratante na execução das seguintes atividades:

- No âmbito de atividades associadas ao fornecimento dos serviços de comunicações;
- No âmbito de atividades associadas à utilização e manutenção de servidores virtuais;
- No âmbito do aluguer de equipamentos;
- No âmbito do fornecimento de serviços de caixas de e-mail.

Caso o subcontratante pretenda realizar alguma alteração técnica ou de outro cariz, deve notificar atempadamente o responsável pelo tratamento, sempre que a mesma interfira com o tratamento de dados pessoais realizado no âmbito do presente contrato.

B.2. Segurança do tratamento

O nível de segurança deverá ter em consideração:

- As categorias de dados pessoais tratadas, incluindo dados de saúde, de filiação sindical e dados de natureza altamente pessoais, como sejam os dados relativos à vida íntima do titular de dados, onde se incluem dados socioeconómicos e de contexto familiar, bem como dados que caracterizam a situação de vulnerabilidade social do titular;
- As categorias de titulares de dados afetados, incluindo-se, mas não se limitando, a trabalhadores;

- Ao contexto da esfera íntima e privada, mesmo que inerente a uma relação laboral, da partilha de informação entre elementos do responsável pelo tratamento, bem como entre o responsável pelo tratamento e terceiros;
- O tratamento de dados pessoais envolve todos os dados que sejam tratados no contexto das atividades do responsável pelo tratamento, enquanto órgão autárquico.

O subcontratante deverá ser intitulado e ter a obrigação de tomar decisões relativas a medidas de segurança técnicas e organizativas que são aplicadas (e alvo de acordo) para implementar um nível de segurança adequado.

O subcontratante deverá, no entanto, - face a qualquer evento e num mínimo – implementar, pelo menos, as medidas tidas como obrigatórias que constam na Resolução do Conselho de Ministros n.º 41/2018:

Requisitos técnicos mínimos das redes e sistemas de informação (conforme a Resolução de Ministros n.º 41/2018)

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

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	Não é permitida a utilização de credenciais em <i>plain text</i> , quer no código quer em ficheiros de configuração	Recomendado.	Obrigatória
	App	Deve ser evitado palavras-passe embebidas no código.	Recomendado.	Obrigatória
	App	As credenciais que necessitem de ser armazenadas em ficheiros de configuração devem estar codificadas (HASH — mínimo SHA 256).	Recomendado.	Facultativa
	BD	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.	Obrigatória
	BD	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.	Obrigatória
Capacidade para autenticar e autorizar	FE	O processo de autenticação deve ser sempre iniciado e mantido em sessão segura.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações	FE	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 (<i>Double Factor Authentication-2FA</i>), como por exemplo: Palavra-passe + SMS Token Palavra-passe + <i>Smartcard</i> 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.	Facultativa
	FE	Dados pessoais de sessão excluídos das variáveis <i>Uniform Resource Locator</i> (URL) ou de outras variáveis visíveis ao utilizador.	Obrigatório.	Obrigatória
	FE	Credenciais de início de sessão transmitidos através do seu HASH, mínimo <i>Secure Hash Algorithm-256</i> (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.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	FE	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 carácter de «espaço».	Obrigatório.	Obrigatória
	FE	Recomenda-se que para novos sistemas seja sempre usado como padrão de autenticação o 2FA.	Recomendado.	Facultativa
	App	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 carácter de «espaço».	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	Para todos os administradores deve-se utilizar Padrão de autenticação 2FA: Exemplos: Palavra-passe + <i>Smartcard</i> Palavra-passe + Biometria Palavra-passe + certificado (por exemplo X.509, da ITU-T para ICP, válido por período não superior a 2 anos).	Obrigatório.	Obrigatória
	App	Como mecanismo de proteção e segurança da informação recomenda-se o uso de <i>Token</i> .	Recomendado.	Facultativa
	App	Comunicação com camadas FE ou BD através de sessão segura, com prévia autenticação se camadas forem física ou logicamente distintas.	Obrigatório.	Obrigatória
	App	Deve ser evitado palavras-passe embebidas no código. Quando tal não for possível, devem estar codificadas (HASH, mínimo SHA-256).	Recomendado.	Obrigatória
	App	Se possível, usar certificados através de API, não sendo desta forma necessário o uso de palavras-passe.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Atribuição de direitos de acesso e privilégio de forma restrita e controlada	App	Autenticação de elementos comunicantes garantida por validação de informação estática ao nível da rede. Exemplos: 1) utilização de IP fixo + <i>hostname</i> + <i>MacAddress</i> + fatores de autenticação, ou 2) Utilização de certificados.	Obrigatório.	Obrigatória
	BD	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 carácter de «espaço».	Obrigatório.	Obrigatória
	BD	Dados pessoais de autenticação, transmitidos através do seu HASH (mínimo SHA-256), ou recorrendo à cifra ou codificação para efetuar essa transmissão.	Recomendado.	Facultativa
	FE	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 (<i>Create</i> , <i>Read</i> , <i>Update</i> , <i>Delete</i> — CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória

Requisito geral		Área	Requisitos Específicos	Classificação	Implementação
	FE		Criação de registo de acesso, alteração e remoção (<i>logs</i>), 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.	Obrigatória
	App		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.	Obrigatória
	App		Criação de registo de acesso, alteração e remoção (<i>logs</i>) 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.	Obrigatória
	BD		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.	Obrigatória
	BD		Criação de registo de acesso, alteração e remoção (<i>logs</i>), 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.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Atribuição das credenciais de acesso de forma controlada através de um processo formal de gestão do respetivo ciclo de vida	FE	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Obrigatória
	FE	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.	Obrigatória
	App	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Obrigatória
	App	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.	Obrigatória
	BD	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	BD	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.	Obrigatória
	FE	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.	Obrigatória
Revisão de direitos de acesso de utilizadores em intervalos regulares	FE	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.	Obrigatória
	FE	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa
	FE	Deve ser desativada uma conta de utilizador quando o mesmo não tem atividade sobre a conta durante 3 meses.	Recomendado.	Facultativa
	App	Processo de gestão de validade de perfis.	Obrigatório.	Obrigatória
	App	Processo de gestão de validade de perfis automatizado.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	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.	Obrigatória
	App	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa
	BD	Processo de gestão de validade de perfis.	Obrigatório.	Obrigatória
	BD	Processo de gestão de validade de perfis automatizado.	Recomendado.	Facultativa
	BD	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.	Obrigatória
	BD	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados	FE	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.	Obrigatória
	FE	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa
	FE	Ação dos utilizadores sobre dados pessoais (CRUD) deve permitir a sua auditoria em registo de atividade (<i>logs</i>).	Obrigatório.	Obrigatória
	App	Para Administradores de Sistemas, Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório.	Obrigatória
	App	Processo de gestão de validade de contas de utilizadores.	Obrigatório.	Obrigatória
	App	Processo de gestão de validade de contas de utilizadores automatizado.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	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.	Obrigatória
	App	Recomenda-se: 1) uma periodicidade bimestral; ou 2) quando se verifique uma alteração no mapa de pessoal associado a esta função.	Recomendado.	Facultativa
	App	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa
	BD	Para Administradores de Bases de Dados, Administradores de Sistemas, de Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório.	Obrigatória
	BD	Processo de gestão de validade das contas dos utilizadores.	Obrigatório.	Obrigatória
	BD	Processo de gestão de validade das contas dos utilizadores automatizado.	Recomendado.	Facultativa
	BD	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Restrição de acesso à informação baseado no princípio necessidade de conhecer (criação de perfil)	FE	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.	Obrigatória
	App	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.	Obrigatória
	App	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.	Obrigatória
	BD	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.	Obrigatória

Requisito geral		Área	Requisitos Específicos	Classificação	Implementação
		BD	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.	Obrigatória
Automatização dos processos de concessão, revisão, análise e revogação de acesso			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.	Obrigatória
Procedimentos seguros de início de sessão			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.	Obrigatória
Capacidade de monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis			Deve ser guardado registo de atividade (<i>log</i>) de todas as ações que um utilizador efetue sobre dados pessoais, independentemente do seu perfil e função.	Obrigatório.	Obrigatória
			Todos os registos de atividade (<i>log</i>) 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.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
		Deve ser guardado registo de atividade (<i>log</i>) de todos os acessos e tentativas falhadas de acesso, obedecendo aos requisitos anteriores.	Obrigatório.	Obrigatória
		Garantir que os registos de atividade provenientes dos diversos subsistemas (Sistemas Operativos, aplicações, <i>browsers</i> , Sistema de Gestão de Base de Dados — SGBD, etc.) são inequivocamente associados à sua origem.	Obrigatório.	Obrigatória
		Os registos de atividade (<i>log</i>) 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 (<i>TimeStamp</i>) da ação, alteração efetuada sobre o dado pessoal.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional		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 na <i>firewall</i>, <i>Intrusion Detection System</i> — 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 <i>Virtual Private Network</i> (VPN).	Obrigatório.	Obrigatória
	FE	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.	Obrigatória
	FE	Recomenda-se as práticas recomendadas em <i>Open Web Application Security Project</i> (OWASP).	Recomendado.	Obrigatória
	FE	Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
		acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.		
	App	Camada aplicacional segregada da rede ou ambiente com visibilidade e/ou acesso exterior.	Obrigatório.	Obrigatória
	App	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.	Obrigatória
	BD	Camada de BD segregada da rede ou ambiente com visibilidade/acesso exterior.	Obrigatório.	Obrigatória
	BD	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.	Obrigatória
	BD	Mascaramento, anonimização ou, sendo necessário, cifra dos dados pessoais transmitidos ou acedidos.	Obrigatório.	Obrigatória
	BD	Dados armazenados (incluindo os existentes em volumes de salvaguarda — <i>backups</i>) devem ser cifrados e assinados digitalmente.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	BD	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.	Facultativa
Capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados pessoais		Deve ser garantida a integridade das zonas <i>Domain Name System</i> (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, <i>Sender Policy Framework</i> — SPF, <i>DomainKeys Identified Mail</i> — DKIM, <i>Domain-based Message Authentication, Reporting and Conformance</i> — DMARC, entre outros).	Obrigatório.	Obrigatória
		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.	Facultativa
Os sistemas de armazenamento devem garantir redundância e		A arquitetura de processamento e armazenamento deve garantir as propriedades da redundância, resiliência e disponibilidade.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
disponibilidade, não devendo existir nenhum « <i>single point of failure</i> »		Devem existir dois tipos de backups (<i>online</i> e <i>offline</i>), que devem obedecer aos mesmos requisitos de segurança definidos para os sistemas produtivos.	Obrigatório.	Obrigatória
		Os backups <i>offline</i> 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.	Obrigatória
		Os sistemas devem estar capacitados para classificar, priorizar, pesquisar, editar e apagar os dados pessoais.	Obrigatório.	Obrigatória
As redes e sistemas de informação devem possuir as funcionalidades necessárias ao respeito pelos direitos do titular dos dados		Os sistemas devem possuir os controlos necessários que permitam a identificação, autenticação, acesso e validação dos dados pessoais armazenados.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
As tecnologias de informação a implementar devem permitir a portabilidade e a exportação de dados pessoais		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.	Obrigatória
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		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.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
		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.	Obrigatória

B.3. Prestação de assistência ao responsável pelo tratamento

O subcontratante deverá, na medida do possível, - atendendo ao âmbito e à extensão da assistência infra especificada - prestar assistência ao responsável pelo tratamento de acordo com as cláusulas 8.1 e 8.2 através da implementação das seguintes medidas técnicas e organizativas:

- O subcontratante deverá designar um ponto de contacto para a Gestão do Projeto associado à prestação dos serviços previstos no presente documento, comunicando-o por e-mail ao Gestor de Contrato do Responsável pelo Tratamento;
- O ponto de contacto do subcontratante deverá disponibilizar um e-mail e um contacto telefónico;
- Deverá existir um contacto alternativo ao ponto de contacto designado para a Gestão de Projeto por parte do subcontratante;
- Qualquer pedido de informação ou comunicação realizada pelo responsável pelo tratamento para o subcontratante deverá ter como período máximo de resposta uma semana.

B.4. Período de armazenamento/procedimentos de apagamento

Após cessação da prestação de serviços de tratamento de dados pessoais, o subcontratante deverá devolver os dados pessoais de acordo com a cláusula 10.1., a menos que o responsável pelo tratamento – após assinatura do contrato – tenha modificado a sua escolha inicial. Tal modificação deverá ser documentada e mantida por escrito, incluindo o formato eletrónico, em conexão com as cláusulas.

B.5. Localização do tratamento

O tratamento de dados pessoais realizado sob aplicação das cláusulas não poderá ser realizado noutras localizações além das pertencentes ao subcontratante, sem a permissão prévia por escrito do responsável pelo tratamento.

B.6. Instrução para a transferência de dados pessoais para países terceiros

A presente prestação de serviços não contempla a transferência de dados pessoais para um país terceiro ou organização internacional.

B.7. Procedimentos para a realização de auditorias pelo responsável pelo tratamento, incluindo inspeções, do tratamento de dados pessoais realizados pelo subcontratante em nome do responsável pelo tratamento

Caso assim o responsável pelo tratamento o entenda por conveniente, poderão ser realizadas auditorias e/ou inspeções ao subcontratante. Tal será realizado mediante comunicação prévia ao subcontratante, com um período de antecedência de 30 dias.

O subcontratante deverá disponibilizar os recursos necessários para que o responsável pelo tratamento possa realizar a auditoria e/ou inspeção.

Os encargos decorrentes da realização da auditoria e/ou inspeção ficam a cargo do responsável pelo tratamento.

O responsável pelo tratamento poderá designar um auditor independente/externo para a realização dos procedimentos supra descritos.