AUTORIDADE NACIONAL DE COMUNICAÇÕES (ANACOM)

DIREÇÃO-GERAL DE GESTÃO DE PESSOAS E DE RECURSOS FINANCEIROS

DIREÇÃO-GERAL DE INFORMAÇÃO E INOVAÇÃO

CONCURSO PÚBLICO
AQUISIÇÃO DA SOLUÇÃO PORTAL DE SERVIÇOS DA ANACOM

CADERNO DE ENCARGOS

NOVEMBRO 2022

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Concurso público

Aquisição da solução Portal de Serviços da ANACOM

Parte I

Condições Gerais

Capítulo I – Disposições gerais

Capítulo II – Obrigações contratuais

Secção I – Obrigações do prestador de serviços

Subsecção I – Disposições gerais

Subsecção II – Dever de sigilo

Subsecção III – Prevenção de conflito de interesses

Parte I
Condições gerais

Capítulo I
Disposições gerais

Cláusula 1.ª

Apresentação

A entidade adjudicante é a Autoridade Nacional de Comunicações (ANACOM), pessoa coletiva de direito público, com natureza de entidade administrativa independente, dotada de autonomia administrativa, financeira e de gestão, bem como de património próprio, com sede em Lisboa, na Avenida José Malhoa, n.º 12.

Cláusula 2.ª

Objeto

O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto principal a aquisição da solução Portal de Serviços da ANACOM, para cumprimento do estabelecido no Regulamento (UE) 2018/1724 do Parlamento Europeu e do Conselho, de 2 de outubro de 2018.

Cláusula 3.ª

Contrato

1 - O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2 - O contrato a celebrar integra ainda os seguintes elementos:
   a) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo Conselho de Administração da ANACOM;
   b) Os esclarecimentos e as retificações relativos ao caderno de encargos;
   c) O presente caderno de encargos;
   d) A proposta adjudicada;
   e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3 - Em caso de divergências entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.

4 - Em caso de divergências entre os documentos referidos no n.º 2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos (CCP) e aceites pelo adjudicatário, nos termos do disposto no artigo 101.º desse mesmo diploma legal.

Cláusula 4.ª

Preço

O preço base para efeitos do presente procedimento pré-contratual é de 200 000 (duzentos mil) euros.

Cláusula 5.ª

Prazo do contrato

O contrato mantém-se em vigor até à conclusão e aceitação dos serviços em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

Capítulo II

Obrigações contratuais

Secção I

Obrigações do prestador de serviços

Subsecção I

Disposições gerais

Cláusula 6.ª

Obrigações principais do prestador de serviços

1 - Sem prejuízo de outras obrigações previstas na legislação aplicável, no caderno de encargos ou nas cláusulas contratuais, da celebração do contrato decorre para o prestador de serviços a obrigação de exata e pontual execução dos serviços adjudicados, de acordo com o previsto no presente caderno de encargos e na proposta adjudicada.

2 - O prestador de serviços fica obrigado a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação dos serviços, bem como ao estabelecimento, monitorização e aperfeiçoamento do sistema de

organização necessário à perfeita e completa execução das tarefas a seu cargo, de acordo com o previsto no presente caderno de encargos.

3 - A deteção de situações anómalas no âmbito da prestação dos serviços obriga à sua comunicação imediata à entidade adjudicante, sendo o prestador de serviços responsabilizado pelas consequências da sua não comunicação imediata.

Cláusula 7.ª

Prazo da prestação dos serviços

1 - O prestador dos serviços obriga-se a concluir a execução dos serviços, com todos os elementos referidos na Parte II do presente caderno de encargos, no prazo máximo de seis meses, a contar da data de outorga do contrato.

2 - O prazo previsto no número anterior pode ser prorrogado por iniciativa da ANACOM ou a requerimento do prestador dos serviços, devidamente fundamentado, e após acordo entre as partes.

Cláusula 8.ª

Local da prestação dos serviços

1 - Os serviços objeto do presente concurso serão prestados nas instalações do prestador de serviços, com exceção dos serviços em relação aos quais, atenta a sua natureza, a ANACOM entenda que devam ser realizados nas suas próprias instalações.

2 - Para os efeitos do disposto na parte final do ponto anterior, o prestador dos serviços compromete-se a cumprir com a prestação dos serviços objeto do presente convite, quer nas atuais da sede da ANACOM, quer ainda noutras instalações da ANACOM, em caso de deslocalização da sua sede para morada diferente da indicada, dentro do concelho de Lisboa.

Cláusula 9.ª

Forma de prestação dos serviços

1 - O prestador de serviços obriga-se a executar os serviços objeto do contrato a outorgar de acordo com os requisitos indicados nas especificações técnicas, da parte II do presente caderno de encargos.

2 - O prestador de serviços deverá basear as suas operações nas melhores práticas de mercado no que respeita à gestão de serviço, utilizando metodologias reconhecidas, para que se obtenha uma elevada eficácia nos serviços a prestar.

3 - O prestador dos serviços fica obrigado a entregar à ANACOM toda a documentação descrita nas especificações técnicas, da parte II do presente caderno de encargos, designadamente:

- Plano de Projeto;
- Definição da Solução;
- Especificação de Requisitos Funcionais;
- Especificação de Requisitos Tecnológicos, o qual terá de incluir a especificação de migração/importação de dados;
- Especificação de Interfaces, o qual terá de incluir: sistemas cliente e sistemas *backend*; parâmetros de entrada e resposta; contrato; segurança de acesso associada; calendário; data de disponibilização do *mock service*; data de disponibilização da integração (pode ter dependências para sistemas terceiros ainda em desenvolvimento);
- Manual de Instalação e Administração ou Manual de configuração.

4 - O prestador dos serviços assegurará ainda a transferência de conhecimentos técnicos e funcionais, antes da entrada em produção da solução, nos termos descritos nas especificações técnicas, da parte II do presente caderno de encargos.

Cláusula 10.ª

Equipa

1 - Para a realização dos serviços objeto do contrato o prestador de serviços afetará os elementos identificados na sua proposta, de acordo com os perfis referidos nas especificações técnicas, da parte II do presente caderno de encargos.

2 - Na eventualidade de o prestador de serviços se ver obrigado a substituir, no decorrer do projeto, qualquer um dos elementos identificados na proposta, esta substituição terá de ser efetuada por outro elemento de perfil equivalente ou superior.

3 - Por motivos justificados, e devidamente fundamentado, a ANACOM poderá requerer a substituição de elementos integrantes da equipa do prestador dos serviços.

4 - A eventual substituição de qualquer um dos elementos identificados na proposta terá sempre de ser comunicada previamente à ANACOM, de cuja autorização dependerá sempre essa substituição, avaliada à luz do perfil apresentado.

Cláusula 11.ª

Inspeção e testes

1 - Com a conclusão dos serviços objeto do contrato, a ANACOM, por si, procede, no prazo de 30 (trinta) dias, à respetiva análise e à realização de testes, com vista a verificar se os mesmos reúnem as características, especificações e requisitos técnicos definidos nas especificações técnicas da parte II do presente caderno de encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.

2 - Durante a presente fase, o prestador dos serviços deve prestar à ANACOM toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar durante a realização daqueles, através de pessoas devidamente credenciadas para o efeito.

3 - Com a conclusão dos testes objeto da presente cláusula, proceder-se-á à sua aceitação provisória, nos termos da cláusula 14.ª do presente caderno de encargos, sem prejuízo do disposto na cláusula seguinte.

Cláusula 12.ª

Inoperacionalidade, defeitos ou discrepâncias

1 - No caso de a análise e os testes previstos na cláusula anterior não comprovarem a total operacionalidade dos serviços objeto do contrato a outorgar, bem como a sua conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos na parte II do presente caderno de encargos, a ANACOM deve disso informar, por escrito, o prestador dos serviços.

2 - No caso previsto no número anterior, o prestador dos serviços deve proceder, à sua custa e no prazo razoável que for determinado pela ANACOM, às alterações e complementos necessários para garantir o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.

3 - Após a realização das alterações e complementos necessários pelo prestador dos serviços, no prazo respetivo, a ANACOM procede à realização de novos testes de aceitação, nos termos da cláusula anterior.

Cláusula 13.ª

Entrada e apoio em produção

1 - Com a aceitação da solução, o prestador dos serviços compromete-se a colocar e apoiar a entrada em produção da solução objeto do presente caderno de encargos.

2 - Após a solução entrar em produção, e verificando-se o cumprimento integral dos requisitos funcionais, técnicos e outros requisitos constantes das especificações técnicas do anexo II do caderno de encargos e da Proposta, proceder-se-á à sua aceitação, nos termos da cláusula seguinte.

Cláusula 14.ª

Aceitação provisória

Caso os testes a que se refere a cláusula 11.ª comprovem a total operacionalidade dos serviços objeto do contrato, bem como a sua conformidade com as exigências legais, e neles não sejam detetadas quaisquer defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos na parte II do presente caderno de encargos, a ANACOM procederá, no prazo de 30 (trinta) dias, à sua aceitação provisória.

Cláusula 15.ª

Garantia técnica

1 - Nos termos da presente cláusula e da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, o prestador dos serviços garante os serviços objeto do contrato a outorgar, pelo prazo de dois anos a contar da data da aceitação provisória, contra quaisquer defeitos ou discrepâncias com as exigências legais e com características, especificações e requisitos técnicos definidos na parte II do presente caderno de encargos, que se revelam a partir da respetiva aceitação dos serviços objeto do presente contrato.

2 - A garantia prevista no número anterior abrange:
   a) o fornecimento, a montagem ou a integração de quaisquer peças ou componentes em falta;
   b) a desmontagem de peças, componentes ou bens defeituosos ou discrepantes;

c) a reparação ou a substituição das peças, componentes ou bens defeituosos ou discrepantes;
d) o fornecimento, a montagem ou instalação das peças, componentes ou bens reparados ou substituídos;
e) o transporte do bem ou das peças ou componentes defeituosos ou discrepantes para o local da sua reparação ou substituição e a devolução daqueles bens a entrega das peças ou componentes em falta, reparados ou substituídos;
f) a deslocação ao local da instalação ou de entrega;
g) a mão-de-obra.

3 - No prazo máximo de dois meses a contar da data em que a ANACOM tenha detetado qualquer defeito ou discrepância, este deve notificar o fornecedor, para efeitos da respetiva reparação.

4 - A reparação, correção ou substituição previstas na presente cláusula devem ser realizadas dentro dos prazos previstos na cláusula seguinte.

Cláusula 16.ª

Níveis de serviço

1 - Durante o período de garantia referido na cláusula anterior deverão ser considerados os níveis de serviço para correções, por nível de criticidade:

Níveis de Serviço corretivo Garantia e Manutenção	
Criticidade	Tempo Máximo de Resolução (horas úteis)
Gravidade Extrema	08 Horas
Gravidade Elevada	16 Horas
Gravidade Média	32 Horas
Gravidade Baixa	64 Horas

2 - Para os efeitos do disposto no ponto anterior, entende-se por:

- gravidade extrema - quando a ANACOM considere crítica a afetação da situação de exploração normal do serviço e a organização é afetada a nível global;
- gravidade elevada - quando a ANACOM considere alta a afetação da situação de exploração normal do serviço e uma unidade funcional é afetada;

- gravidade média - quando a ANACOM considere média a afetação da situação de exploração normal do serviço e vários utilizadores são afetados;
- gravidade baixa - quando a ANACOM considere baixa a afetação da situação de exploração normal do serviço e apenas o utilizador que reporta o incidente é afetado.

Cláusula 17.ª

Aceitação definitiva

Findo o período de garantia referido na cláusula anterior, e encontrando-se a Plataforma em boas condições de operacionalidade, de conformidade e de funcionamento, proceder-se-á à sua aceitação definitiva.

Cláusula 18.ª

Transferência da propriedade

1 - Com a aceitação a que se refere a cláusula anterior, ocorre a transferência da posse e da propriedade do Portal e dos elementos a desenvolver ao abrigo do contrato para a ANACOM, incluindo os direitos autorais sobre as criações intelectuais abrangidas pelos serviços a prestar.

2 - Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente caderno de encargos

Subsecção II

Dever de sigilo

Cláusula 19.ª

Sigilo e diligência

1 - O prestador de serviços e os respetivos colaboradores estão sujeitos, nos termos da legislação penal e dos estatutos da ANACOM, a sigilo profissional sobre os factos cujo conhecimento lhes advenha da prestação dos serviços objeto do contrato a celebrar e, seja qual for a finalidade, não podem divulgar nem utilizar, em proveito próprio ou alheio, diretamente ou por interposta pessoa, o conhecimento que tenham desses factos.

2 - O prestador de serviços e os respetivos colaboradores estão igualmente sujeitos a sigilo sobre toda a informação, documentação ou outros elementos de que tenham conhecimento, no âmbito da prestação de serviços objeto do contrato a celebrar.

3 - 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.

4 - Exclui-se do dever de sigilo previsto a informação e a documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo prestador de serviços, e pelos seus colaboradores, ou que estes sejam legalmente obrigados a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

5 - Sem prejuízo da responsabilidade civil e criminal que dela resulte, a violação do sigilo pelo prestador de serviços e pelos seus colaboradores prevista na presente cláusula, confere à ANACOM o direito a resolver imediatamente o contrato sem qualquer contrapartida para a outra parte.

6 - O prestador de serviços e os respetivos colaboradores estão ainda sujeitos ao dever de diligência sobre todos os assuntos que lhes sejam confiados.

Cláusula 20.ª

Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor indefinidamente, até autorização expressa em contrário pela ANACOM, a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Subsecção III

Prevenção de conflitos de interesses

Cláusula 21.ª

Prevenção de conflitos de interesses

O prestador de serviços declara sob compromisso de honra que:

1 - Não mantém, nem manterá, direta ou indiretamente, qualquer vínculo ou relação contratual, remunerada ou não, com empresas, grupos de empresas ou outras entidades destinatárias da atividade reguladora da ANACOM **que possam originar conflitos de interesses** na prestação dos serviços abrangidos pelo contrato a celebrar, durante a vigência do mesmo, nos termos e para os efeitos do artigo 43.º dos

Estatutos da ANACOM, aprovados pelo Decreto-Lei n.º 39/2015, de 16 de março.

2 - Não detém qualquer participação social ou interesses nas empresas, grupos de empresas ou outras entidades destinatárias da atividade reguladora da ANACOM **que possam originar conflitos de interesses** na prestação dos serviços abrangidos pelo contrato a celebrar, durante a vigência do mesmo, nos termos e para os efeitos do artigo 43.º dos Estatutos da ANACOM, aprovados pelo Decreto-Lei n.º 39/2015, de 16 de março.

3 - Não mantém, nem manterá, direta ou indiretamente, qualquer vínculo ou relação contratual, remunerada ou não, com outras entidades cuja atividade possa colidir com o exercício das atribuições e competências da ANACOM e **que possa originar conflitos de interesses** na prestação dos serviços abrangidos pelo contrato a celebrar, durante a vigência do mesmo, nos termos e para os efeitos do artigo 43.º dos Estatutos da ANACOM, aprovados pelo Decreto-Lei n.º 39/2015, de 16 de março.

4 - Se ao longo da prestação de serviços vier a ocorrer algum facto relevante suscetível de originar conflito de interesses, nos termos acima indicados, compromete-se a informar a ANACOM desse facto e a tomar as medidas necessárias para a sua superação.

Secção II

Obrigações da ANACOM

Cláusula 22.ª

Preço contratual

1 - Pela prestação dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a ANACOM deve pagar ao prestador de serviços o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.

2 - O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à ANACOM, nomeadamente, entre outros, as despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças, bem como de direitos de propriedade intelectual, autoral ou de direitos conexos, decorrentes da incorporação nas atividades objeto do

contrato a outorgar, ou da utilização nessas atividades, de hardware, de software ou outros.

Cláusula 23.ª

Condições de faturação e de pagamento

1 - A quantia devida pela ANACOM deve ser paga no prazo de 30 (trinta) dias após a receção pela ANACOM das respetivas faturas, as quais deverão ser emitidas de acordo com o seguinte plano de faturação:

a) 30% do valor do contrato, acrescido de IVA à taxa legal em vigor, com a entrega, e aceitação pela ANACOM, da Especificação de Requisitos funcionais (DER) e da Especificação de Requisitos Técnicos (DET);

b) 20% do valor do contrato, acrescido de IVA à taxa legal em vigor, com a conclusão, e aceitação pela ANACOM, da especificação de interfaces (DEI) e dos serviços de interoperabilidade;

c) 30% do valor do contrato, acrescido de IVA à taxa legal em vigor, com a conclusão dos testes e a entrada em produção da solução, nos termos da cláusula 11.ª do presente caderno de encargos;

d) 10% do valor do contrato, acrescido de IVA à taxa legal em vigor, com a conclusão dos serviços de Formação, nos termos do disposto na cláusula 9.ª do presente caderno de encargos;

e) 10% do valor do contrato, acrescido de IVA à taxa legal em vigor, com a aceitação provisória, nos termos da cláusula 14.ª do presente caderno de encargos.

2 - Em caso de discordância por parte da ANACOM, quanto aos valores indicados na fatura, deve este comunicar ao prestador de serviços, por escrito, os respetivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

3 - O prestador de serviços deverá cumprir com a legislação em vigor relativa à faturação eletrónica em procedimentos aquisitivos de contratação pública, nomeadamente, entre outras, o disposto no Decreto-Lei n.º 28/2019, de 15 de fevereiro, que regula as obrigações relativas ao processamento de faturas e outros documentos fiscalmente relevantes, e no Decreto-Lei n.º 123/2018, de 28 de dezembro, na versão em vigor que define o modelo de governação para a implementação da faturação eletrónica nos contratos públicos.

4 - A fatura deverá ser compatível com o sistema de faturação eletrónica implementado pela ANACOM.

5 - Para efeitos de cumprimento do referido no parágrafo anterior, será o prestador de serviços devidamente informado pela ANACOM do procedimento a seguir para proceder à faturação dos serviços prestados, mediante pedido de esclarecimento do prestador de serviços, a enviar para o endereço de correio eletrónico infoeletronica@anacom.pt.

6 - Desde que devidamente emitida, e observado o disposto na presente cláusula, a fatura é paga através de transferência bancária, para o IBAN que seja indicado pelo prestador de serviços.

Capítulo III
Penalidades contratuais e resolução do contrato

Cláusula 24.ª
Penalidades contratuais

1 - Pelo incumprimento das obrigações emergentes do contrato a outorgar, a ANACOM pode, a título sancionatório, aplicar as seguintes penalidades:
   a) pelo incumprimento do prazo de realização dos serviços por motivos que sejam imputáveis exclusivamente ao prestador de serviços, 2% do valor global do contrato por cada dia útil de atraso, até um valor máximo acumulado de 20% do valor global do contrato;
   b) pelo incumprimento dos níveis de serviços, 0,5% do valor global do contrato por cada dia útil de atraso, até um valor máximo acumulado de 20% do valor global do contrato.

2 - Em caso de resolução do contrato por incumprimento do prestador de serviços, a ANACOM pode exigir-lhe uma pena pecuniária de até 5% do valor contratual.

3 - Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo prestador de serviços ao abrigo do número 1, relativamente aos serviços cujo atraso na respetiva conclusão tenha determinado a resolução do contrato.

4 - Na determinação da gravidade do incumprimento, a ANACOM tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa (dolo ou negligência) do prestador de serviços e as consequências do incumprimento.

5 - A ANACOM pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.

6 - As penas pecuniárias previstas na presente cláusula não obstam a que a ANACOM exija uma indemnização pelo dano excedente.

Cláusula 25.ª

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 força maior, se se verificarem 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 sociedade 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 apenas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 26.ª

Resolução do contrato por parte da ANACOM

1 - Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, a ANACOM pode resolver o contrato, a título sancionatório, no caso de o prestador de serviços violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, nomeadamente o incumprimento das obrigações resultantes do contrato a outorgar ou a sua prossecução deficiente e/ou reiterada, designadamente:
   a) atraso não justificado superior a 10 (dez) dias na conclusão dos serviços objeto do contrato a outorgar;
   b) não resolução das não conformidades ou discrepâncias mencionadas no n.º 1 da cláusula 12.ª, no prazo de cinco dias após o prazo determinado pela ANACOM mencionado no n.º 2 da mesma cláusula.

2 - Nos termos e ao abrigo do disposto no artigo 5.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro, o direito de resolução referido no parágrafo primeiro da presente cláusula exerce-se mediante declaração a enviar pela ANACOM ao prestador de serviços para o endereço de correio eletrónico do gestor (ou responsável) do contrato do prestador de serviços, ou para o endereço de correio eletrónico a facultar pelo prestador de serviços para os efeitos do disposto no presente caderno de encargos, respeitante às comunicações e notificações entre as partes.

3 - O direito de resolução referido no parágrafo primeiro da presente cláusula não determina a repetição das prestações já realizadas, a menos que tal seja determinado pela ANACOM.

4 - A resolução do contrato pela ANACOM não prejudica o dever de o adjudicatário indemnizar a ANACOM pelos eventuais prejuízos resultantes das situações previstas no parágrafo primeiro da presente cláusula, nem a possibilidade de aplicação das penalidades mencionadas no presente caderno de encargos.

Cláusula 27.ª

Resolução do contrato por parte do prestador de serviços

1 - Sem prejuízo de outros fundamentos de resolução previstos na lei, o prestador de serviços pode resolver o contrato quando qualquer montante que lhe seja devido esteja em dívida há mais de seis meses ou quando o montante em dívida exceda 25% do preço contratual, excluindo juros.

2 - O direito de resolução é exercido mediante declaração enviada à ANACOM, que produz efeitos 30 (trinta) dias após a receção dessa declaração, salvo se esta última cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.

3 - A resolução do contrato nos termos dos números anteriores não determina a repetição das prestações já realizadas pelo prestador de serviços, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444.º do CCP.

Capítulo IV
Resolução de litígios

Cláusula 28.ª

Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do tribunal administrativo de círculo de Lisboa, com expressa renúncia a qualquer outro.

Capítulo V
Disposições finais

Cláusula 29.ª

Subcontratação e cessão da posição contratual

1 - A subcontratação e a cessão da posição contratual por qualquer das partes regem-se nos termos e ao abrigo do disposto no artigo 316.º e seguintes do CCP.

2 - O prestador de serviços não poderá subcontratar, total ou parcialmente, qualquer uma das obrigações que para si decorrem do contrato a outorgar sem o consentimento prévio e escrito da ANACOM.

3 - A subcontratação de qualquer entidade por parte do prestador de serviços não o desvinculará de qualquer responsabilidade ou obrigação para si decorrente do contrato a outorgar.

4 - O prestador de serviços não poderá ceder a sua posição contratual, total ou parcialmente, qualquer uma das obrigações que para si decorrem do contrato a outorgar sem o consentimento prévio e escrito da ANACOM.

Cláusula 30.ª

Gestor do contrato

Será nomeado um gestor do contrato por parte da ANACOM, com a função de acompanhamento permanente da execução do contrato.

Cláusula 31.ª

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 CCP, preferencialmente, para os endereços de correio eletrónico dos gestores (ou responsáveis) pelo contrato designados por cada parte, ou para o domicílio ou sede contratual de cada uma, identificadas no contrato.

2 - Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 32.ª

Contagem dos prazos

Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados.

Clausula 33.ª

Legislação aplicável

O contrato é regulado pela legislação portuguesa.

O Diretor-Adjunto
da Direção-Geral de Gestão de Pessoas
e de Recursos Financeiros

PARTE II

Especificações técnicas

Portal de Serviços ANACOM

1 INTRODUÇÃO

O REGULAMENTO (UE) 2018/1724 DO PARLAMENTO EUROPEU E DO CONSELHO, doravante referido apenas como "Regulamento" relativo à criação de uma Plataforma Digital Única - Single Digital Gateway, visa facilitar o acesso em linha às informações, procedimentos administrativos e serviços de assistência de que os cidadãos e empresas necessitam para poder deslocar-se na União Europeia, comercializar produtos, estabelecer-se e expandir atividades noutro Estado Membro.

Para cumprimento integral do estabelecido neste regulamento, conjugado com o Regulamento de execução (UE) 2020/1121 da comissão de 29 de julho de 2020, doravante referido apenas como "Regulamento de execução", a ANACOM pretende implementar um portal, designado Portal de Serviços ANACOM, no âmbito do qual deverão ser facilitadas as interações entre os cidadãos e as empresas, por um lado, e as autoridades competentes, por outro, concedendo acesso a soluções em linha, facilitando as atividades quotidianas dos cidadãos e das empresas e minimizando os obstáculos encontrados no mercado interno. A existência deste portal com acesso em linha a informações exatas e atualizadas e a procedimentos e serviços de assistência e de resolução de problemas poderá sensibilizar os utilizadores para os diferentes serviços existentes em linha, permitindo-lhes poupar tempo e dinheiro.

Com a implementação deste portal, os benefícios esperados são:

- reduzir os encargos administrativos adicionais para os cidadãos e para as empresas que exercem ou desejam exercer os seus direitos no mercado interno, incluindo a livre circulação dos cidadãos, no pleno respeito das regras e dos procedimentos nacionais;
- eliminar a discriminação entre cidadãos nacionais e transfronteiriços; e
- garantir o funcionamento do mercado interno no que diz respeito à prestação de informações, de procedimentos e de serviços de assistência e de resolução de problemas.

2 OBJETIVOS

Desenvolvimento de um Portal, para cumprimento de 3 objetivos:

1. a prestação de informações;
2. a disponibilização de procedimentos integralmente em linha e
3. o acesso a serviços de assistência e de resolução de problemas.

3 ÂMBITO

Desenvolvimento de um Portal, incluindo:

- Backoffice;
- Frontend;
- Desenvolvimento de serviços de interoperabilidade com serviços/sistemas internos e externos à ANACOM

4 NOTA METODOLÓGICA

Os requisitos estão identificados da seguinte forma:

RFn - requisitos funcionais da solução.

RDMn - Requisitos de desenvolvimento e manutenção.

RPn - Requisitos da proposta.

Em que n = número do requisito.

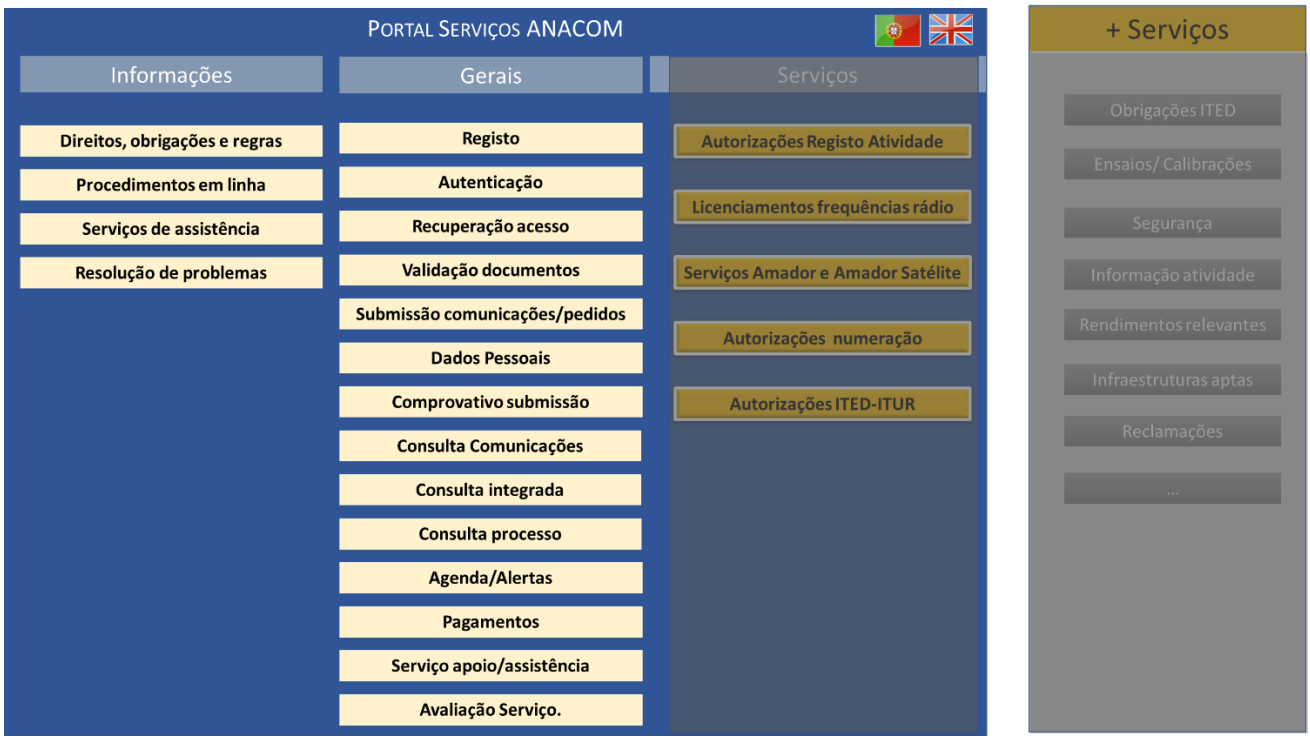
A proposta a apresentar deve cumprir:

RP1. Terá de indicar explicitamente por cada requisito, na matriz de conformidade em anexo A, a descrição do cumprimento do requisito, sendo que a ANACOM não considerará as meras transcrições de partes deste documento, com exceção dessa exigência para o presente RP1.

5 REQUISITOS DA SOLUÇÃO

5.1 FUNCIONALIDADES

O PORTAL SERVIÇOS ANACOM disponibiliza as funcionalidades transversais (informações e gerais), conforme figura seguinte.



5.1.1 INFORMAÇÕES

RF1. Disponibilização de conteúdos, com gestão pelo utilizador, para informação, notícias, perguntas e respostas frequentes, em formato texto, vídeo, imagem, infografia e hiperligação, incluindo download de dados, ajuste de formato, mapeamento e visualização de tabelas e gráficos.

5.1.2 REGISTO E AUTENTICAÇÃO

RF2. Registo de novo utilizador, através de utilizador/senha, chave móvel digital, cartão de cidadão, certificado digital, autenticação europeia (eIdas).

RF3. Credenciação de utilizador (atribuição de poder de representação)

RF4. Recuperação de acesso (utilizador/senha)

RF5. Autenticação de utilizador, incluindo poderes de representação, quando aplicável.

5.1.3 DADOS PESSOAIS

RF6. Gestão, por parte do próprio utilizador, dos seus dados de identificação e de contacto, para pessoa singular e coletiva.

RF7. Atualização de dados pessoais por verificação com os dados do cartão de cidadão.

RF8. Garantia das funcionalidades relacionadas com a proteção de dados pessoais, em conformidade com o disposto no Regulamento (UE) 2016/679 e com a legislação e regulamentação nacionais aplicáveis.

5.1.4 FORMULÁRIOS E DOCUMENTOS

RF9. Submissão de comunicações ou pedidos através do preenchimento de formulários e anexação de ficheiros (texto, imagem, áudio ou vídeo).

RF10. Geração de pdf, com informação submetida, com *QR Code* e código de validação, para disponibilização ao utilizador, no Portal e/ou canal indicado.

RF11. Validação e apresentação de documentos, por leitura de *QR Code* ou código de validação, com apresentação do documento e dados.

RF12. Informação de apoio à submissão de comunicações ou pedidos através do preenchimento de formulários e à entrega de documentos e ferramentas de ajuda contextual.

RF13. Emissão automática de comprovativos de submissão de comunicações ou pedidos e de entrega de documentos, incluindo data e hora da apresentação, número de registo e, quando aplicável, prazo de resolução.

RF14. Disponibilização de ligação para acesso direto às páginas/formulários, garantindo a autenticação, quando aplicável.

RF15. Análise da informação e método para exportação da informação para o ePortugal (https://eportugal.gov.pt/). Pretende-se exportar dados de texto e hiperligações, para formato excel, a pedido do utilizador.

5.1.5 FUNCIONALIDADES EM AMBIENTE RESERVADO

RF16. Acesso, consulta e geração de documento com as interações entre a ANACOM e o utilizador, independentemente do canal utilizado.

RF17. Consulta integrada de dados e de processos relativos ao utilizador, apresentada numa vista sistematizada por contextos de negócio.

RF18. Consulta aos processos relativos ao utilizador, incluindo o respetivo estado.

RF19. Apresentação de agenda e de alertas, quando aplicável por contexto de negócio.

RF20. Emissão de alertas no Portal e noutros canais indicados pelo utilizador (SMS ou email).

5.1.6 SERVIÇO DE PAGAMENTO

RF21. Gerar referência de pagamento.

RF22. Atualizar informação a partir de notificação de pagamento.

5.1.7 LÍNGUAS

RF23. Versão integral em Português e Inglês, exceto no *Backoffice*.

RF24. Adaptação automática da língua tendo em conta informação relacionada com o utilizador.

RF25. Alteração da língua a pedido.

5.1.8 SERVIÇO DE ATENDIMENTO

RF26. Serviço de atendimento através de formulário e *chat* com assistente virtual e real. A adoção da solução para o assistente virtual estará dependente de análise a realizar em sede de projeto.

RF27. Disponibilização de recursos de inteligência que detetem dificuldades na utilização da informação ou de funcionalidades por parte do utilizador e que reencaminhem para o serviço de atendimento.

5.1.9 BACKOFFICE

RF28. Consultar e descarregar (download) formulários e documentos submetidos pelos interessados.

RF29. Estruturar para disponibilização de conteúdos no Portal.

RF30. Gestão de utilizadores.

RF31. Edição dos textos das interfaces gráficas de utilizador, nomeadamente ajudas, notas, tooltips, mensagens.

RF32. Carregar (upload) documentos e comunicações recebidas ou enviadas por outros canais (e.g. correio postal ou eletrónico).

RF33. Atualizar estado de pedidos, usando lista de valores pré-definidos.

RF34. Efetuar o registo de pedidos.

RF35. Organizar por ordem cronológica (i) a listagem de pedidos e (ii) em cada pedido a listagem de interações com possibilidade de consulta direta dos documentos associados.

RF36. Pesquisar pedidos e documentos.

RF37. Enviar notificações associadas ao pedido.

RF38. Definir diferentes tipos de respostas tipo, utilizando templates configuráveis.

RF39. Classificar, através de lista de valores disponíveis, os diferentes conteúdos.

5.1.10 DADOS ESTATÍSTICOS

RF40. Implementação de ferramenta para recolha de feedback (reação utilizador), registar anonimamente qualidade e a disponibilidade dos serviços prestados através da plataforma, das informações nela disponibilizadas e da interface comum do utilizador.

RF41. Recolher e apresentar dados estatísticos sobre os utilizadores e sobre as suas reações sobre os serviços da plataforma de acordo com o estabelecido nos artigos 24.º e 25.º do REGULAMENTO (UE) 2018/1724 DO PARLAMENTO EUROPEU E DO CONSELHO de 2 de outubro de 2018 e no REGULAMENTO DE EXECUÇÃO (UE) 2020/1121 DA COMISSÃO de 29 de julho de 2020.

5.1.11 GESTÃO DE UTILIZADORES

RF42. Criar, eliminar e configurar perfis.

RF43. Atribuir e remover perfis a um ou mais utilizadores.

RF44. Implementar, pelo menos, os seguintes perfis:

- Utilizador Funcional: privilégios de acesso para leitura e escrita. Este perfil terá de ser subdividido em vários perfis funcionais, de acordo com as responsabilidades de cada perfil funcional no processo de trabalho;
- Responsável Funcional ANACOM: privilégios de manutenção de perfis de utilizador para poder atribuir e remover perfis a um ou mais utilizadores. Tem privilégios para configurar os parâmetros funcionais no sistema;
- Administrador de sistemas: privilégios para assumir a administração tecnológica (bases de dados, software e hardware). Configura os parâmetros da infraestrutura para funcionamento do sistema no momento da instalação ou alterações;
- Responsável da entidade externa: privilégios de manutenção de perfis de utilizador para poder atribuir e remover perfis a um ou mais utilizadores da sua entidade.

5.2 INTEROPERABILIDADE

RDM 1. No desenvolvimento do Portal, âmbito do presente procedimento, devem ser cumpridas as normas descritas no Regulamento Nacional de Interoperabilidade Digital.

5.2.1 SISTEMAS INTERNOS

RDM 2. Implementação de um serviço para atualizar o pedido, que será consumido pelos sistemas que tratam o pedido.

RDM 3. Implementação de serviços para registar comunicações (dados e/ou documentos) estabelecidas noutros sistemas.

RDM 4. Disponibilizar estrutura de dados estatísticos para utilização por outros sistemas internos.

RDM 5. Integração com ERP para gerir informação sobre pagamentos.

RDM 6. Integração com o sistema de gestão documental *através de utilização de serviços*.

5.2.2 SISTEMAS EXTERNOS

RDM 7. Autenticação - Autenticação com Cartão Cidadão (CC) e Chave Digital Móvel (CDM), incluindo atributos profissionais, através da integração com serviços da iAP | plataforma de interoperabilidade da administração pública, disponibilizada pela Agência para a Modernização Administrativa, I.P. (AMA). Documentação disponível em https://github.com/amagovpt/.

RDM 8. Autenticação europeia – integração com serviços eIDAS | Plataforma de interoperabilidade da Comissão Europeia, disponibilizada pela AMA.

RDM 9. A solução deve garantir a autenticação e a autorização de acesso através de *Single-Sign-On* (SSO) com ePortugal.

RDM 10. Integração com serviços da iAP | plataforma de pagamentos – PPAP, para obtenção de informação relativa a pagamentos, disponibilizada pela AMA.

RDM 11. Integração com serviços IRN relativos a ficheiro central pessoas coletivas.

RDM 12. Integração com o SPNE (Serviço público de notificações eletrónicas), disponibilizada pela AMA.

RDM 13. Integração com a Gateway de SMS (GAP), disponibilizada pela AMA.

RDM 14. Integração com a Interoperabilidade Documental, disponibilizada pela AMA.

RDM 15. Transmitir dados estatísticos sobre os utilizadores sobre as suas reações de acordo com o estabelecido nos artigos 24.º e 25.º do REGULAMENTO (UE) 2018/1724 DO PARLAMENTO EUROPEU E DO CONSELHO de 2 de outubro de 2018 e no REGULAMENTO DE EXECUÇÃO (UE) 2020/1121 DA COMISSÃO de 29 de julho de 2020.

RDM 16. Integrar G*oogle Analytics* para recolha de métricas gerais de acesso, perfil de utilizador, etc, bem como Events Analytics, que suportados em dashboards de gestão (data studio), vão permitir identificar oportunidades de melhoria contínua do serviço.

RDM 17. Integração com o sistema técnico para o intercâmbio automatizado transfronteiriço de elementos de prova e aplicação do princípio da declaração única de acordo com o estabelecido no artigo 14.º do REGULAMENTO (UE) 2018/1724 DO PARLAMENTO EUROPEU E DO CONSELHO de 2 de outubro de 2018.

5.3 TRATAMENTO DE DADOS PESSOAIS

O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, doravante designado RGPD, veio introduzir um novo regime em matéria de proteção de dados pessoais.

Para além do reforço da proteção jurídica dos direitos dos titulares dos dados, o RGPD exige novas regras e procedimentos do ponto de vista tecnológico.

RDM 18. De modo a cumprir as normas do RGPD, implementar na solução os mecanismos de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais, conforme estabelecido na Resolução do Conselho de Ministros n.º 41/2018 para a Administração Pública.

5.4 MIGRAÇÃO

RDM 19. Deverá ser assegurada a migração dos dados dos cerca de 14000 utilizadores (pessoa singular e coletiva) registados atualmente em base de dados Oracle. O processo de migração será estabelecido em sede de projeto.

5.5 INFRAESTRUTURA TECNOLÓGICA DE SUPORTE À SOLUÇÃO A IMPLEMENTAR

RDM 20. Deverá apresentar a arquitetura da solução identificando e justificando a utilização de cada componente/produto.

RDM 21. A solução deverá ser totalmente Microsoft, suportada na infraestrutura cloud Azure.

RDM 22. A ANACOM dispõe Microsoft Dynamics 365 Customer Service para gestão da relação com as entidades externas, pelo que os desenvolvimentos previstos no presente procedimento deverão ter em conta esta realidade.

RDM 23. Todas as integrações com os sistemas terceiros serão implementadas, pela equipa de integração da ANACOM, na plataforma de integração - IPaaS da Azure – AZURE Integration Services.

5.6 INTERFACES E EXPERIÊNCIA DE UTILIZAÇÃO

A disposição gráfica geral e as principais soluções de navegação serão entregues em sede de projeto.

RDM 24. Cumprir o Decreto-lei n.º 83/2018, de 19 de outubro, que transpõe a Diretiva (UE) 2016/2102 do Parlamento Europeu e do Conselho, relativa à acessibilidade dos sítios Web e das aplicações móveis.

RDM 25. O Portal terá de cumprir os requisitos de usabilidade e acessibilidade, em alinhamento com as linhas gerais e imagem do design system da AMA (https://github.com/amagovpt/; https://zeroheight.com/1be481dc2/p/97181d-gora-design-system).

RDM 26. Devem ser seguidas as recomendações constantes do portal http://usabilidade.gov.pt.

RDM 27. Cumprir o Acordo Ortográfico em vigor (AO1990).

RDM 28. Cumprir o Anexo B – Regras de escrita da ANACOM.

RDM 29. Todos os serviços devem ser *responsive* de modo a oferecer uma experiência de utilização adequada a quem utilize um computador, tablet ou smartphone.

5.7 SEGURANÇA

RDM 30. Cumprir com o regime jurídico da segurança do ciberespaço, de modo a garantir um elevado nível comum de segurança dos sistemas de informação.

6 TESTES DO SISTEMA

RDM 31. Deverão ser entregues os seguintes planos de testes e respetivos relatórios com resultados obtidos:

a. Testes globais - validação do funcionamento e coerência global do sistema e dos respetivos dados;
b. Testes funcionais - validação individual de cada funcionalidade descrita no desenho técnico e implementada no sistema;
c. Testes de integração - validação da comunicação e troca de informação com os sistemas externos ao sistema com a qual este terá de comunicar, incluindo a simulação de situações de erro de comunicação;
d. Testes de carga ou desempenho - validação da capacidade do sistema de responder em tempo útil, e em ambiente de produção, ao nível de utilização esperado;
e. Testes de segurança - validação dos pressupostos de segurança assumidos e deteção de fragilidades de segurança passíveis de serem utilizados por técnicas de ataque conhecidas;
f. Testes de usabilidade e acessibilidade- meios que comprovem a realização de testes de Usabilidade/acessibilidade com utilizadores (relatório de testes ou vídeo ou fotografias, etc.), que demonstrem o cumprimento dos requisitos.

7 METODOLOGIA E FASEAMENTO

A gestão de projetos de Sistemas e Tecnologias de Informação na ANACOM segue um modelo organizacional PMO (Project Management Office ou, Escritório de Projetos de Sistemas de Informação).

Deverá ser identificada e descrita a metodologia de gestão de projetos a usar.

RP2. Terá de apresentar e descrever as diversas etapas da metodologia de gestão de projeto.

RP3. Terá de apresentar a metodologia de gestão de alterações de âmbito.

RP4. Deverá apresentar um cronograma detalhado das respetivas atividades e documentos a entregar, relativos à gestão de projeto e à solução.

RP5. Terá de garantir na proposta a entrega do Plano de Projeto e os entregáveis:

- Definição da Solução;
- Especificação de Requisitos Funcionais;
- Especificação de Requisitos Tecnológicos, o qual terá de incluir a especificação de migração/importação de dados;
- Especificação de Interfaces, o qual terá de incluir: sistemas cliente e sistemas *backend*; parâmetros de entrada e resposta; contrato; segurança de acesso associada; calendário; data de disponibilização do *mock service*; data de disponibilização da integração (pode ter dependências para sistemas terceiros ainda em desenvolvimento).
- Manual de Instalação e Administração ou Manual de configuração;

RP6. Atendendo a que a ANACOM dispõe do produto Microsoft DevOps, a entrega de informação da solução deverá ser neste suporte.

RP7. Terá de providenciar os meios necessários para que, durante qualquer fase do projeto, a ANACOM possa auditar o cumprimento das metodologias, processos e procedimentos de gestão da qualidade do processo e do produto.

RP8. A fase de testes a realizar no ambiente QA deve ser precedida por uma demonstração da solução à Equipa de Projeto e à Equipa de Testes de Aceitação ANACOM, em QA.

RP9. Terá de garantir que os procedimentos de desenvolvimento e entrega da solução cumprem o normativo de segurança e interoperabilidade na implementação de soluções de Software, em anexo C ao caderno de encargos.

8 EQUIPA DO PROJETO

A Equipa de projeto é composta por membros da ANACOM e da empresa contratada (Fornecedor).

RP10. Terá de indicar na proposta o perfil e a experiência dos elementos da Equipa do prestador dos serviços que participam nas tarefas-.

RP11. Requisitos mínimos de experiência dos membros da equipa:

Perfil	Experiência
Gestão de projeto - Experiência em Gestão de Projetos similares, em complexidade tecnológica e dimensão.	Mínimo 5 anos
Técnico – Experiência no desenvolvimento de soluções baseadas em tecnologias Microsoft: Power Platform, Dynamics 365, Azure.	Mínimo 3 anos

9 FORMAÇÃO

RP12. Terá de assegurar a transferência de conhecimentos técnicos e funcionais relativos aos produtos de projeto antes da entrada em produção

Anexo A

MATRIZ DE CONFORMIDADE DOS REQUISITOS

Preencha a matriz indicando as páginas da proposta em que descreve os requisitos RFn, RDMn e RPn e a forma de os cumprir.

Identificação do Requisito (ex: RF1)	Página de resposta	Descrição do cumprimento

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Anexo B

REGRAS DE ESCRITA

Índice

1. Nota introdutória

Na sequência da deliberação do Conselho de Administração (CA), de 19 de Maio de 2011, sobre a implementação do novo Acordo Ortográfico (AO) na ANACOM, foram revistas as regras de escrita que os colaboradores devem seguir na elaboração de conteúdos de comunicação interna e externa, tais como: publicações institucionais, deliberações, relatórios, memorandos, decisões e projectos de decisão e documentos de consulta.

Os principais objectivos subjacentes à elaboração destas linhas de orientação, são:

a) uniformizar o formato e a imagem dos diversos documentos de comunicação interna e externa da ANACOM;
b) alinhar os *templates* de texto da ANACOM com cada suporte de comunicação, por forma a tirar maior partido das suas especificidades e potencialidades;
c) facilitar a produção de documentos, permitindo que o tempo despendido pelos colaboradores da ANACOM seja dedicado maioritariamente à preparação do respectivo conteúdo e não à forma do documento.

2. Formatação do documento

2.1. Tipo de letra

- Fonte: Arial.
- Tamanho: 11 pt.
- Estilo: normal.

2.2. Espaçamentos e alinhamento

- Espaçamento entre linhas: 1,5 linhas.
- Espaçamento entre parágrafos: 12 pt antes e 6 pt depois.
- Alinhamento do texto: justificado.

2.3. Margens

- Superior: 4 cm.
- Inferior: 2,5 cm.
- Esquerda: 3 cm.

- Direita: 2,5 cm.

2.4. Cabeçalho e rodapé

- Dimensão: 1,25 cm.
- Cabeçalho: título do documento, alinhado à esquerda (Arial, 9 pt, normal)[1].
- Rodapé: numeração da página, alinhada à direita (Arial, 9 pt, normal).

3. Regras específicas

3.1. Títulos e subtítulos

Os títulos e subtítulos devem ser curtos, concisos e apelativos, exprimindo o essencial do capítulo ou da parte do documento a que dizem respeito.

- Títulos principais:
  - tipo de letra: Arial, 12 pt, negrito;
  - espaçamento entre linhas: 1,5 linhas;
  - espaçamento entre parágrafos: 12 pt antes e 6 pt depois.
- Títulos secundários ou subtítulos:
  - tipo de letra: Arial, 11 pt, negrito;
  - espaçamento entre linhas: 1,5 linhas;
  - espaçamento entre parágrafos: 12 pt antes e 6 pt depois.
- Numeração: os títulos e subtítulos devem ser numerados, recorrendo a numeração árabe e decimal, não devendo contudo ser excedida a 4.ª ordem (ex.: 1., 1.1., 1.1.1., 1.1.1.1.).
- Maiúsculas: apenas a primeira palavra dos títulos e subtítulos deverá surgir com letra maiúscula inicial, com exceção dos casos gramaticalmente previstos (ex.: nomes próprios, continentes, países, cidades, etc.).

[1] Não aplicável a todo o tipo de documentos.

3.2. Numeração e *bullets*

Pode-se numerar ou recorrer a *bullets* nos parágrafos. No caso da numeração será utilizado um dos dois seguintes estilos: "a, b, c, …" ou "i, ii, iii, …".No caso dos *bullets*, será utilizado um dos seguintes estilos: "▪", "•" ou "-".

No final de cada *bullet*/parágrafo numerado deve ser utilizado o ";", iniciando-se o bullet/parágrafo seguinte com letra minúscula ou com ".", caso em que se iniciará o bullet/parágrafo seguinte com maiúscula.

O último *bullet*/parágrafo numerado deve terminar sempre com ".".

3.3. Figuras (gráficos, tabelas, esquemas, etc.)

As figuras devem ser claras e compreensíveis, tanto na impressão a cores como a preto e branco, referindo, quando aplicável, as unidades e a fonte dos dados apresentados.

Deverão ser editáveis, não sendo por isso inseridas no documento com formato de imagem.

É desejável que se destaquem os aspectos mais relevantes, recorrendo, por exemplo, a cores diferentes ou à utilização de negritos.

Nos gráficos com barras ou colunas, estas devem ser apresentadas em sequência lógica (ordem crescente/decrescente ou ordem temporal).

Os detalhes desnecessários deverão ser eliminados, nomeadamente através do arredondamento dos valores para uma casa decimal e do agrupamento dos *itens* de menor expressão numa categoria "outros" ou "diversos", se for viável e não prejudicar o que se pretende evidenciar.

Os gráficos e tabelas relacionados entre si devem ser colocados na mesma página, para facilitar a leitura comparativa, podendo as figuras mais extensas ser colocadas em apêndice ou em anexo.

- Título:
  - tipo de letra: Arial, 9 pt, negrito;
  - espaçamento entre linhas: 1,5 linhas;
  - espaçamento entre parágrafos: 12 pt antes e 3 pt depois;

- localização: fora da figura, por cima e alinhado à esquerda;
- numeração: de forma sequencial, com numeração própria e árabe (evitar numeração 1.x).

- Fonte dos dados:
  - tipo de letra: Arial, 8 ou 7 pt, normal;
  - espaçamento entre linhas: 1 linha;
  - espaçamento entre parágrafos: 3 pt antes e 12 pt depois;
  - localização: fora da figura, por baixo e do lado esquerdo.
- Legendas:
  - tipo de letra: Arial, 9 pt, normal;
  - localização: por baixo da figura e centradas, com exceção da *pie* em que ficará do lado direito.
- Unidades:
  - tipo de letra: Arial, 9 pt, normal;
  - localização: por baixo do gráfico, antes da fonte, alinhada à esquerda.

Nas tabelas os dados serão alinhados à direita e separados por uma coluna branca. Os totais serão destacados em baixo.

3.4. Corpo de texto

- Formatação:
  - tipo de letra: Arial, 11 pt, normal;
  - espaçamento entre linhas: 1,5 linhas;
  - espaçamento entre parágrafos: 12pt antes e 6 pt depois;
  - alinhamento do texto: justificado.
- Itálicos: utilizar apenas para as expressões em latim ou língua estrangeira (salvo o nome de pessoas, organizações e localidades, que não devem constar em itálico). Em inglês, as expressões em itálico devem ser igualmente utilizadas sempre que se trate de uma língua estrangeira (diferente do inglês e português).
- Aspas: utilizar apenas para as citações.
- Siglas: não levam pontos e não fazem plural (ex. de sigla incorrecta: “PALOP’s”), sendo que na primeira menção no documento deverá sempre constar a

designação por extenso com a sigla entre parêntesis [ex.: Países Africanos de Língua Oficial Portuguesa (PALOP)]. Nas menções seguintes em pontos ou capítulos subsequentes, basta recorrer à sigla correspondente.

Quando se trabalha numa versão em inglês, convém ter presente que algumas as siglas diferem do português [ex. PT – União Europeia (UE); EN – European Union (EU)].

- Maiúsculas: devem ser apenas utilizadas no início de frases, em nomes próprios ou siglas, seguindo a regra gramatical e evitando a tendência de usar maiúsculas sem critério, a meio de um texto. Exceção: a palavra Internet mantém a maiúscula.
- Negrito e sublinhado: não utilizar palavras a negrito ou sublinhado no corpo do texto, excepto quando existirem razões que o aconselhem.
- Notas de rodapé:
  - tipo de letra: Arial, 9 pt, normal;
  - espaçamento entre linhas: 1 linha;
  - espaçamento entre parágrafos: 3 pt antes e depois;
  - alinhamento do texto: justificado;
  - localização: as notas de rodapé são sempre colocadas sequencialmente e no fundo da página, terminando com um ponto final, com espaço entre o número e o início do texto e a duas colunas (português à esquerda e correspondente tradução na coluna da direita.).
- Números: A Norma Portuguesa n.º 9/2006 (relativa à escrita dos números), do Instituto Português da Qualidade, prescreve o seguinte:

  "2. Princípios

  2.1. A vírgula é exclusivamente destinada a separar, nos números, a parte inteira da parte decimal (ex.: "10,3").

  2.2. Os números serão escritos em grupos de três algarismos a partir das unidades, quer para a esquerda, quer para a direita (parte decimal).

  Exemplos: 32 048 21 237,459 32

2.3. Os grupos de três algarismos, tanto da parte inteira como da parte decimal, se ela existir, devem ser separados por um espaço igual ao ocupado por qualquer dos algarismos, no caso da escrita dactilográfica, e um pouco inferior, no caso da impressão.

Portanto, deve-se escrever:

1 437 385,327 61

e não 1.437.385,327.61, nem 1437385,327661.

3. Excepções

Os princípios atrás expostos não se aplicam à parte inteira ou à parte decimal no caso de as mesmas serem formadas só por quatro algarismos, salvo quando os números são escritos em coluna.

Exemplos:

a) 1437,327 61 e 14 373,2761

b) 5 321,003 4
1 465,005 35
3 679,002 1
10 465,010 85 "

- Os números não podem ser separados, pelo que, caso tal aconteça na mudança de linha, torna-se necessário arrumar o texto, de modo a que fiquem sempre juntos.
- Na versão inglesa estas normas são diferentes, com os milhares separados por vírgulas (ex. "13,500" e "13,500,250") e as casas decimais por pontos (ex. "20.9").
- A abreviatura de número é "n.º".
- Escrever centenas de milhares e não centenas de milhar.
- Se os números citados forem superiores ao milhão podem escrever-se as centenas numericamente e os milhares ou milhões por extenso.
- Nunca escrever bilião, mas sim mil milhões.

- Moedas: a designação de moedas, no corpo de texto, deve ser escrita por extenso e com letra minúscula (ex.: "100 euros"). O símbolo do euro (€) ou a sigla EUR deverá ser utilizado apenas em quadros, gráficos ou figuras, colocado depois do montante e separado por um espaço. Esta regra aplica-se a todas as línguas, com exceção do inglês em que o símbolo vem antes do montante.

- Medidas:

  - em regra, no corpo de texto, as medidas devem ser escritas por extenso (ex.: "10,3 por cento" ou "350 quilómetros"), evitando-se a utilização de símbolos (% ou KM), geralmente reservada a contextos estatísticos (gráficos e tabelas);
  - neste caso, os símbolos escrevem-se com letra minúscula (excepto quando têm origem em nomes próprios) e são colocados à direita dos números e com um espaço a intervalar (ex.: "25 km" ou "3,5 kg");
  - faixas de frequências: podem utilizar-se os respectivos símbolos, devendo ser escritas de forma a não existir espaços entre os números e o hífen, mas com um espaço entre o número e a medida (ex.: "700-720 kHz").

- Símbolos:

  - em regra, os símbolos escrevem-se com letra minúscula (excepto quando têm origem em nomes próprios) e são colocados à direita dos números e com um espaço a intervalar (ex.: "25 km" ou "3,5 kg");
  - símbolo do euro (€): deverá ser colocado à direita do número e separado por um espaço (100 €);
  - símbolo de percentagem (%): deverá ser colocado à direita do número e sem espaço entre o número e o símbolo (ex.: "10%");
  - símbolos de tempo: o símbolo de hora(s) é "h", de minuto(s) é "min" e de segundo(s) é "s", podendo ser igualmente utilizada a representação dos relógios digitais (ex: A reunião terá início às 15:00 e deverá durar até às 18:30.).

- Data:

  - a data deve ser escrita com o dia em primeiro lugar, seguido do mês e, por último, o ano, devendo o primeiro e o último elemento ser escritos em numeração árabe (ex.: "11 de Abril de 2007");

- pode utilizar-se a representação abreviada da data representada por DD.MM.AAAA (ex. "11.04.2007"). A separação deve ser feita por "." e não por qualquer outro símbolo como por exemplo "-" ou "/";
- referências temporais entre duas datas escrevem-se assim: 1990-94 ou 1990-2010, caso envolvam dois séculos;
- quando se trata de um período que abrange dois anos – 1990-1991.

▪ Abreviaturas:

- escreve-se a primeira letra seguida de ponto (s. – substantivo) ou a primeira sílaba e a primeira letra da segunda sílaba seguidas de ponto (arc. – arcaico). Caso a primeira letra da segunda sílaba seja vogal, deve escreve-se até à próxima consoante (neol. – neologismo);
- devem eliminar-se pelo menos 3 letras da expressão original;
- todas as abreviaturas devem terminar com ponto e quando se utilizam várias abreviaturas seguidas, estas devem ser separadas por um espaço (p. ex.);
- quando a palavra abreviada estiver no fim do período, este encerra-se com o ponto abreviativo pois não se coloca outro ponto depois dele;
- a abreviatura de "primeiro, segundo e terceiro" deve corresponder a "1.º, 2.º e 3.º";
- alguns exemplos:

Abrev.	Eng.ª	i. e.	Pág.
Art.º	Etc.	Lda.	Págs.
Av.	Exa.	N.º	S. A.
D. L. n.º	Exmo.	Obs.	Sr.
Eng.º	Fig.	p. ex.	Sr.ª

▪ Nomes e designações:

- a sigla ICP-ANACOM não pode ser separada em contexto algum. Quando na translineação ICP e ANACOM ficam separados, torna-se necessário arrumar o texto, de modo a que a sigla apareça sempre junta;

- na designação de entidades (ex.: operadores e prestadores), na primeira vez que são referenciadas, deve ser usada a designação oficial completa e, entre parêntesis, a sigla com a designação reduzida correspondente [ex.: "PT Comunicações, S. A. (PTC)" ou "Vodafone Portugal – Comunicações Pessoais, S. A. (Vodafone)]. A partir daí, deve ser utilizada a sigla (PTC), a não ser que alguma razão específica aconselhe a repetição da designação completa. A designação é redigida em minúsculas, excepto nos casos em que a designação oficial envolve uma sigla como PT Comunicações ou AR Telecom, caso em que "PT" e "AR" se redigem em maiúsculas;
- a designação dos países que pertencem à União Europeia (UE) deve corresponder a "Estados-Membros", enquanto a dos países que integram outras organizações intergovernamentais deve corresponder a "Estados Membros" (ex.: "Estados Membros da União Internacional das Telecomunicações"), "Partes" ou outra designação que seja aplicável na organização em causa, nomeadamente por força do que tenha sido adoptado na tradução oficial que suporta o respectivo instrumento de ratificação;
- a designação das organizações internacionais, nomeadamente aquelas em que a ANACOM participa, deve constar em português, tal como a sigla correspondente [ex.: União Internacional das Telecomunicações (UIT)].

- Informação confidencial: a informação que não pode ser revelada deve ser ~~apagada~~, mantendo-se todavia o espaço ocupado pela mesma para que a versão pública corresponda na íntegra à versão confidencial. No início deste espaço em branco deve ser inserido a indicação de «Inicio de Informação Confidencial (IIC)» e no fim «Fim de Informação Confidencial (FIC)». Nos espaços seguintes já poderão ser utilizadas estas siglas.
- Indicação de *links*: A indicação das páginas dos *sites* onde se encontram documentos citados no corpo do texto deve ser feita em notas de rodapé, colocadas sequencialmente e no fundo da página (com espaço entre o número e o início do texto e terminando com um ponto final).

4. Palavras com dupla grafia

As palavras com dupla grafia deverão ser escritas de acordo com a grafia tradicional, ou seja, tal como se leem na primeira coluna da tabela abaixo (p. ex. sector e espectro).

Lista de palavras com dupla grafia

GRAFIA TRADICIONAL	NOVA GRAFIA
acupunctor	acupuntor
acupunctura	acupuntura
acupuncturação	acupunturação
acupunctural	acupuntural
acupuncturar	acupunturar
anti-infeccioso	anti-infecioso
apocalíptico	apocalítico
aquapunctura	aquapuntura
aquapuncturar	aquapunturar
aspecto	aspeto
aspectual	aspetual
asséptico	assético
assimptota	assintota
carácter	caráter
cardiopunctura	cardiopuntura
circunspecto	circunspeto
conceptáculo	concetáculo
conceptibilidade	concetibilidade
conceptismo	concetismo
conceptista	concetista
conceptístico	concetístico
conceptiva	concetiva
conceptível	concetível
conceptual	concetual
conceptualismo	concetualismo
conceptualista	concetualista
conceptualístico	concetualístico
conceptualização	concetualização
conceptualizar	concetualizar
conceptualmente	concetualmente
conectividade	conetividade
conector	conetor

GRAFIA TRADICIONAL	NOVA GRAFIA
conectora	conetora
consumpção	consunção
consumptibilidade	consuntibilidade
consunptível	consumtível
consunptivo	consumtivo
contráctil	contrátil
contractilidade	contratilidade
contractível	contratível
contractivo	contrativo
contracto	contrato
contractura	contratura
contracturante	contraturante
dactilofasia	datilofasia
dactilógrafa	datilógrafa
dactilografado	datilografado
dactilografar	datilografar
dactilografia	datilografia
dactilográfico	datilográfico
dactilógrafo	datilógrafo
dactilograma	datilograma
dactilologia	datilologia
dactilológico	datilológico
dactilonomia	datilonomia
dactiloscopia	datiloscopia
dactiloscópico	datiloscópico
dactilozoário	datilozoário
deflectir	defletir
deflectível	defletível
deflector	defletor
deíctica	deítica
dêictica	dêitica
deíctico	deítico
dêictico	dêitico
didactologia	Didatologia

GRAFIA TRADICIONAL	NOVA GRAFIA
didactológico	didatológico
eclíptica	eclítica
eclíptico	eclítico
eréctil	erétil
erectilidade	eretilidade
espectador	espetador
espectral	espetral
espectro	espetro
espectrofobia	espetrofobia
espectrofotometria	espetrofotometria
espectrofotométrico	espetrofotométrico
espectrofotómetro	espetrofotómetro
espectrografia	espetrografia
espectrográfico	espetrográfico
espectrógrafo	espetrógrafo
espectrograma	espetrograma
espectrologia	espetrologia
espectrológico	espetrológico
espectrometria	espetrometria
espectrométrico	espetrométrico
espectrómetro	espetrómetro
espectroscopia	espetroscopia
espectroscópico	espetroscópico
espectroscópio	espetroscópio
espetroscopista	espectroscopista
estupefactivo	estupefativo
expectação	expetação
expectador	expetador
expectante	expetante
expectar	expetar
expectativa	expetativa
expectatório	expetatório
expectável	expetável

GRAFIA TRADICIONAL	NOVA GRAFIA
fotorreceptor	fotorrecetor
fototactismo	fototatismo
galvanopunctura	galvanopuntura
gliptografia	glitografia
haptotactismo	haptotatismo
hidrotactismo	hidrotatismo
ictérica	itérica
icterícia	iterícia
ictérico	itérico
ignipunctura	ignipuntura
infeccionar	infecionar
infeccioso	infecioso
infecto	infeto
infectocontagioso	infetocontagioso
insectífero	insetífero
insectiforme	insetiforme
insectófilo	insetófilo
insectologia	insetologia
insectológico	insetológico
insetívoro	insectívoro
insetologista	insectologista
intáctil	intátil
intactilidade	intatilidade
intelecção	inteleção
intercepto	interceto
intersecção	interseção
interseccional	intersecional
interseccionismo	intersecionismo
intersectar	intersetar
láctico	lático
liquefacção	liquefação
liquefactivo	liquefativo
multissectorial	multissetorial
narcoléptico	narcolético

GRAFIA TRADICIONAL	NOVA GRAFIA
noctívaga	notívaga
noctívago	notívago
olfactometria	olfatometria
opticidade	oticidade
opticometria	oticometria
opticométrico	oticométrico
percepto	perceto
perfeccional	perfecional
perfeccionismo	perfecionismo
perfeccionista	perfecionista
perfeccionístico	perfecionístico
perfectibilidade	perfetibilidade
perfectibilizar	perfetibilizar
perfectível	perfetível
perfectividade	perfetividade
perfectivo	perfetivo
preceptivamente	precetivamente
preceptivo	precetivo
preceptor	precetor
preceptora	precetora
preceptorado	precetorado
preceptoral	precetoral
preceptoria	precetoria
preceptorial	precetorial
protráctil	protrátil
punctura	puntura
putrefactivo	putrefativo
quimiotactismo	quimiotatismo
rarefactível	rarefatível
rarefactivo	rarefativo
reflectografia	refletografia
reflectográfico	refletográfico
retráctil	retrátil

GRAFIA TRADICIONAL	NOVA GRAFIA
retractilidade	retratilidade
retractivo	retrativo
retracto	retrato
sector	setor
sectorial	setorial
séptico	sético
septuplicar	setuplicar
séptuplo	sétuplo
subsector	subsetor
tacticografia	taticografia
tacticográfico	taticográfico
táctil	tátil
tactilidade	tatilidade
tactilmente	tatilmente
tactismo	tatismo
telespectador	telespetador
termotactismo	termotatismo
tigmotactismo	tigmotatismo
trofotactismo	trofotatismo
venipunctura	venipuntura
veredicto	veredito
zigotactismo	zigotatismo

Anexo C

Segurança e Interoperabilidade na Implementação de Soluções de Software

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Normativo de Segurança e Interoperabilidade na Implementação de Soluções de Software

(v22.04)

Índice

Preâmbulo

O presente documento normativo define regras específicas relativas ao desenvolvimento ou implementação de soluções de software na ANACOM. As regras aqui descritas encontram-se em alinhamento e requerem o estrito cumprimento das recomendações e dos normativos padrão internacionais de organismos como o IETF (Internet Request for Comments – RFCs), ISO/IEC, ITU, IEEE (*e.g.* 802, 1003 series), W3C (CSS3, HTML5), NIST (Special Publication 800 series), OWASP (Open Web Application Security Project – free and open software security community), da legislação comunitária como o Regulamento da União Europeia (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados), assim como da legislação nacional designadamente a Resolução do Conselho de Ministros n.º 41/2018 que define as orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais e em prossecução no mesmo âmbito a Lei n.º 58/2019 que assegura a execução na ordem jurídica nacional do Regulamento (UE) 2019/679, a Resolução do Conselho de Ministros n.º 2/2018 relativa ao Regulamento Nacional de Interoperabilidade Digital (RNID) e a Lei n.º 36/2011 que estabelece a adoção de normas abertas nos sistemas informáticos do Estado.

Conformidade com a Política de Segurança

Regras de segurança e qualidade no desenvolvimento e na implementação de software

A produção e implementação do software deverá ser efetuada considerando o necessário enquadramento com a política de segurança vigente na ANACOM, devidamente endereçando:

- as medidas de segurança, *i.e.* a confidencialidade, integridade e confiabilidade (fiabilidade e disponibilidade), aplicacional, dos repositórios de dados, das credenciais de autenticação, das tokens de sessão, da informação e da respetiva infraestrutura;

- a implementação dos mecanismos de controlo de autenticação e autorização e registo de acessos (logging) e de atividade (accounting), de gestão e proteção das *tokens* de sessão e credenciais de acesso, com recurso aos meios padrão de criptografia, simétrica (chave secreta) e assimétrica (chave pública/privada), aplicados aos repositórios de dados, canais de comunicação e *interfaces* aplicacionais;

- a aplicação das metodologias de Engenharia de Software e de desenvolvimento adequadas ao paradigma em causa que contribuam para a produção de código eficiente e de qualidade. As referidas metodologias devem assegurar que em qualquer contexto durante o processo de desenvolvimento, se detetam e eliminam defeitos e vulnerabilidades, *i.e.* falhas de conceção ou bugs de implementação, entre outros, *use-after-free*, *memory leak*, *heap* ou *stack buffer overflow*, *null pointer dereference*, suscetíveis a ataques (*i.e.* as técnicas utilizadas para exploração de vulnerabilidades) de execução arbitrária de código, negação de serviço DoS, code, command ou SQL injection, XSS, CSRF, SSRF, exfiltração ou adulteração de dados e/ou da informação;

- a validação (input validation) e sanitização das instâncias de dados recebidos, desde parâmetros atuais (argumentos), configuração e variáveis de ambiente, independentemente de onde sejam utilizados (*e.g. headers*, *cookies*, *query strings*, *form fields*) e a utilização de Bind Variables como forma de proteção contra ataques SQL injection. A pré-validação de dados *client-side* não é suficiente nem dispensa a validação efetuada *server-side*;

- a utilização de ferramentas de *code review* e de inspeção e análise estática de código (*linters*) como o Findbugs, o Programming Mistake Detector (PMD) ou a coleção Super-Linter (Azure Pipelines);

- a utilização de ferramentas de gestão de versionamento e *source control*, revision control system;

- a conformidade com as recomendações e os princípios aduzidos na metodologia OWASP (Open Web Application Security Project) com particular atenção para a adoção das recomendações sobre, entre outros, os principais tipos de ataques: SQL Injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), Session hijacking, Clickjacking, Brute Force Attack, Credential stuffing, Command Injection, Code Injection, Buffer Overflow via Environment Variables. Ver também a lista Top 10 Web Application Security Risks.

- a conformidade com os princípios e recomendações de eficiência e desempenho Google PageSpeed Insights;
- a utilização de padrões como o *Java Naming Convention* como base de regras de escrita para as designações de identificadores (Classes, Packages, Interfaces, Methods, Variables, Constants, etc.)
- a implementação dos mecanismos de resiliência necessários para a tolerância a falhas por forma a que a sua ocorrência não afete o correto funcionamento do sistema. Todas as faltas, erros e falhas deverão receber o devido tratamento sendo exigidos mecanismos de *reporting* e depuração de erros adequados à natureza dos mesmos, criando-se assim condições que proporcionem índices mínimos de disponibilidade de classe 5 – Alta Disponibilidade (*i.e.* 99.999%);
- a implementação dos mecanismos necessários de controlo de estado e fluxo e o efetivo tratamento de exceções. Estes devem ainda garantir a não exposição de informação interna em condições de erro;
- a realização de testes unitários que permitam, ao nível dos módulos e componentes básicos do sistema, a deteção de desvios à especificação, realização de testes de integração entre os diferentes módulos e verificação da interação e comunicação entre estes enquanto conjunto, realização de testes funcionais no ambiente, condições e volumes de dados finais, testes de regressão para identificação da reintrodução de *bugs* já anteriormente corrigidos, testes carga para avaliação do desempenho do sistema em condições limite;
- a adoção das especificações standard W3C CSS3 e HTML5 no âmbito das linguagens utilizadas para descrição da semântica de apresentação e de estruturação de documentos web.

Regras de entrega do software

As entregas de software, devidamente versionado e datado em *release*, efetuadas na prossecução de projetos de implementação ou desenvolvimento, de manutenção evolutiva ou corretiva, devem fazer-se acompanhar do respetivo *ChangeLog*, *source code* (aplicável ao software desenvolvido à medida) e *build scripts* necessários à produção do *package* de software entregue e *scripts* SQL (DDL, DML) consolidados e versionados, de implementação da estrutura da camada de persistência de dados (no caso de se tratar da primeira passagem a produção) ou de alteração (cumulativa ou incremental indicando-o) da já existente com os respetivos *scripts* de *Rollback*.

Os *packages release* de software e todos os conteúdos conexos, designadamente os anteriormente referidos, têm de ser assinados digitalmente (PGP/GPG) e disponibilizados, por omissão, no formato tarball ou noutros formatos de *package management systems* mais convenientes no contexto específico do projeto em causa, *e.g.* rpm, npm, pip, etc, em repositórios de código/software ou sistemas de *bug tracking*, internos da ANACOM ou do fornecedor, podendo ser utilizados entre outros: Jira, Maven, Git (*e.g.* GitHub, GitLab, Bitbucket), CPAN (Comprehensive Perl Archive Network), PyPI (Python Package Index), CRAN (Comprehensive R Archive Network).

Regras relativas à documentação do software

A entrega do software tem de ser acompanhada do respetivo manual de instalação. Este manual de instalação deve indicar de forma explícita a versão do manual e do software a instalar, o *ChangeLog* do manual e do software a instalar, a representação esquemática da arquitetura da solução a que corresponde o software, a listagem concisa de todos os componentes a instalar e a sua interdependência com outros referindo o respetivo versionamento, condições e pré-requisitos e a *checklist* com a sequência de instalação. Caso sejam utilizados componentes de terceiros deverá ser anexa ao manual de instalação a matriz previamente aprovada pela ANACOM referida mais à frente neste documento no ponto "Regras de utilização de software *third-party*".

Devem estar descritos claramente todos os procedimentos e ações necessárias a executar no processo de instalação assim como as ações de recuperação em caso de falha do mesmo.

Os manuais de instalação devem ser versionados e datados, assim como o próprio software a instalar, sendo exigido um manual por cada entrega de software, mesmo no caso em que não ocorram alterações aos procedimentos entre versões de software instalado. Neste caso deve ser esse facto indicado no respetivo *ChangeLog* do manual. A entrega da documentação final deve ser efetuada em documentos PDF/A (ISO 19005) com os metadados devidamente sanitizados.

O *ChangeLog* do manual de instalação deve descrever as alterações efetuadas aos procedimentos de instalação ou sobre outra informação que nele conste. O *ChangeLog* relativo ao software deve descrever todas as alterações efetuadas ao próprio.

Regras de classificação de incidentes

As anomalias detetadas no software (*e.g. bugs* e outras desconformidades), são geridas em conformidade com as melhores práticas da *framework* ITIL e o modelo padrão ITSM definido no International Standard ISO/IEC 20000 "Service Management System", devidamente registadas e classificadas como Incidentes Corretivos. Estes incidentes recebem uma classificação de Prioridade calculada automaticamente numa escala graduada em "Baixa", "Média", "Alta" e "Crítica", baseada numa matriz de classificação de Impacto e de Urgência, ambos também definidos na mesma escala. A classificação de Prioridade estabelece o tempo máximo de resolução com base no SLA contratado para a manutenção corretiva.

As definições e metodologias seguidas no âmbito da gestão da manutenção corretiva de software, devem ser conforme o estabelecido no ISO/IEC 14764 Software Engineering "Software Life Cycle Processes - Maintenance".

Regras de classificação de vulnerabilidades

As vulnerabilidades identificadas no *software*, são classificadas como incidentes de segurança em conformidade com o modelo *Common Vulnerability Scoring System* (CVSS). O valor obtido no vetor *CVSS Base Score* que avalia o impacto e estabelece a urgência, será utilizado na classificação do nível de

Prioridade (Incident Priority Matrix conforme a *framework* ITIL) e, decorrente deste, o tempo máximo de resolução com base no SLA contratado para a manutenção corretiva.

Regras de implementação e utilização de Base de Dados

A camada de persistência de dados utilizada pelas soluções a desenvolver ou implementar deve ser suportada em bases de dados (RDBMS) SQL. As funcionalidades e recursos dos motores de base de dados utilizados devem ser standard e independentes de quaisquer implementações específicas (*e.g.* Oracle, Microsoft).

Não deve ser desenvolvido código aplicacional (*e.g.* lógica do negócio) sobre a camada de base de dados (*e.g.* PL/SQL, Java). Devem utilizar-se recursos de abstração e encapsulamento (princípio Encapsulation Layer Architecture) no acesso à camada de persistência de dados (*e.g.* JPA – Java Persistence API, JDO – Java Data Objects).

Devem utilizar-se Connection Pools, Prepared Statements e Bind Variables (nunca string concatenation) como medida de segurança (*e.g.* preventiva de SQL injection), de eficiência e de desempenho. Deve igualmente seguir-se a prática de libertação (close) de qualquer recurso, logo que deixe de ser necessário, recorrendo-se a *try/catch/finally blocks*. A utilização obrigatória de um *finally block* pretende assegurar que a libertação dos recursos ocorre mesmo no caso de ocorrência de exceções (SQL Exception).

Os dados que se estabeleçam inerentemente como sensíveis devem ser encriptados no repositório de base de dados utilizando os recursos próprios do respetivo motor. A comunicação com a base de dados, originada em clientes aplicacionais ou outros, sempre que possível deve ser suportada no protocolo TLS.

As regras e procedimentos de desenho e implementação do modelo de dados encontram-se detalhadas no normativo sobre aplicações e sobre nomenclatura BD.

Regras de disponibilização de serviços HTTP

Os serviços disponibilizados segundo o paradigma Web devem ser suportados nos protocolos HTTP/1.1 (IETF RFC 7230) e HTTP/2 (IETF RFC 7540) sobre o protocolo TLS (HTTPS).

Em termos gerais devem ser seguidas as recomendações do Best Current Practice IETF RFC 7525 "Recommendations for Secure Use of Transport Layer Security (TLS)". Especificamente, devem ser implementadas apenas as versões mais recentes do protocolo TLS v1.3 (IETF RFC 8446) e v1.2 (IETF RFC 5246). Os *cipher suites* a utilizar devem suportar apenas os algoritmos de encriptação (*bulk block encryption algorithms*) **AES 128-bit** e **256-bit GCM** (Galois Counter Mode) [*com opção de fallback para CBC (Cipher Block Chaining) no caso do protocolo TLSv1.2*] e opção **CHACHA20-POLY1305** tanto em TLSv1.3 como em TLSv1.2, os algoritmos *key exchange/agreement* **ECDHE** (*Perfect Foward Secrecy*) baseados apenas em autenticação **RSA**, e ainda os algoritmos de *hashing* (*message digest/authentication*) **SHA 256-bit, 384-bit** ou superior (o SHA-1 160-bit não deve ser utilizado).

Cipher suites TLSv1.2 Server-preferred order

Notação IANA Std.		Notação OpenSSL	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	ECDHE-RSA-AES256-GCM-SHA384	IETF RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	ECDHE-RSA-AES128-GCM-SHA256	IETF RFC 5289
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	ECDHE-RSA-CHACHA20-POLY1305	IETF RFC 7905

Apenas caso exista algum constrangimento, poderão ainda ser utilizados em TLSv1.2:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	*0xc028*	*ECDHE-RSA-AES256-SHA384*	*IETF RFC 5289*
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	*0xc027*	*ECDHE-RSA-AES128-SHA256*	*IETF RFC 5289*
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	*0xc024*	*ECDHE-RSA-AES256-SHA*	*IETF RFC 4492*
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	*0xc023*	*ECDHE-RSA-AES128-SHA*	*IETF RFC 4492*

Cipher suites TLSv1.3 Server-preferred order

Notação IANA Std.		Notação OpenSSL (v1.1)	
TLS_AES_256_GCM_SHA384	0x1302	TLS_AES_256_GCM_SHA384	IETF RFC 8446
TLS_AES_128_GCM_SHA256	0x1301	TLS_AES_128_GCM_SHA256	IETF RFC 8446
TLS_CHACHA20_POLY1305_SHA256	0x1303	TLS_CHACHA20_POLY1305_SHA256	IETF RFC 8446

a) Cipher Suites: key exchange/agreement algorithm = **ECDHE**; authentication = **RSA**; bulk block encryption algorithms = **AES-256-GCM** e **AES-128-GCM** (fallback to AES-256-CBC e AES-128-CBC em TLSv1.2) e **CHACHA20-POLY1305** em opção; message authentication code algorithm = **SHA384** e **SHA256** (server-preferred order).

b) EC Named Curves: **x25519**, secp384r1, secp521r1(server preferred order)

c) Renegotiation: apenas Secure Renegotiation e sem Client-Initiated Renegotiation (aplicável apenas ao TLSv1.2 - o TLSv1.3 não suporta renegociação)

d) TLS compression: sem compressão TLS (imunização do CRIME attack - CVE-2012-4929)

e) HTTP compression: deve utilizar-se para conteúdos estáticos e eventualmente para conteúdos dinâmicos desde que não sejam misturados secrets (*e.g.* tokens CSRF) com user-input refletido no conteúdo produzido dinamicamente (BREACH vulnerability)

Não podem ser utilizados os protocolos SSL v2.0 ou v3.0 (IETF RFC 6176 "Prohibiting Secure Sockets Layer Version 2.0" e RFC 7568 "Deprecating Secure Sockets Layer Version 3.0") nem devem ser suportados os

protocolos TLS v1.0 ou TLS v1.1 (IETF RFC 7525). Não podem ser utilizados algoritmos de encriptação RC4 (IETF RFC 7465 "Prohibiting RC4 Cipher Suites"), DES ou 3DES. Não podem ser utilizados algoritmos MD5.

Na infraestrutura servidora serão implementados os seguintes headers HTTP (mínimo):

Strict-Transport-Security: *max-age=63072000; includeSubDomains; preload*

X-XSS-Protection: *1; mode=block*

X-Frame-Options: *sameorigin*

X-Content-Type-Options: *nosniff*

Content-Security-Policy: *valor a definir durante a implementação - o mínimo será "frame-ancestors 'self'"*

Referrer-Policy: *strict-origin-when-cross-origin*

Set-Cookie: *devem estar sempre presentes as flags Secure e HttpOnly*

Regras de travessia dos perímetros de segurança

A existência zonas de segurança onde residem os diferentes componentes do sistema de informação da ANACOM, impõe regras no que concerne à travessia dos perímetros que as delimitam.

HSZ (High Security Zone)	*Rede interna da ANACOM, onde residem as infraestruturas dos principais serviços (e.g. base de dados, Integration Server, Web Services)*	Pode iniciar ligações para a DMZ
DMZ (Demilitarized Zone)	*Rede externa, exposta à Internet, onde residem as infraestruturas dos serviços front-end*	Pode iniciar ligações para a HSZ apenas através de mecanismos mediadores

Nota: Início da ligação refere-se ao TCP SYN. Uma vez estabelecida a ligação, o fluxo da comunicação é bidirecional.

Na comunicação entre as diferentes zonas de segurança são utilizados *forward* e/ou *reverse web proxies* para integração com *web services ou gateways* de desacoplamento de serviços, a residir na HSZ ou na DMZ, sendo estes os únicos pontos de contacto entre a rede externa e a rede interna.

A comunicação deverá ser suportada em *web services* utilizando o protocolo HTTPS (HTTP over TLS) para encapsulamento e transporte dos protocolos WSDL/SOAP, REST em XML ou JSON sobre HTTP utilizando a plataforma de integração SOA Enterprise Service Bus (ESB). Como poderão existir limitações quanto ao fluxo das mensagens, poderá ser necessário implementar uma comunicação assíncrona ou *plesiócrona* entre ambos, considerando os mecanismos de validação que assegurem o controlo do fluxo e de estado.

Estas interfaces devem suportar e oferecer *per si* os mecanismos necessários e suficientes para garantir a confidencialidade e integridade das comunicações, repositórios e respetivos conteúdos assim como de resiliência e consistência devendo assegurar a recuperação de erros e falhas. Pretende-se que todos os processos que tenham de atravessar o perímetro de segurança, estejam suportados no mesmo meio, eliminando quaisquer processos *ad-hoc* de sincronização entre a DMZ e a HSZ, que coloquem constrangimentos à política de segurança.

Caso na solução a desenvolver ou a implementar existam requisitos de integração com sistemas aplicacionais externos à ANACOM, deverá sempre e sem prejuízo de outros requisitos, utilizar-se o protocolo TLS (HTTPS), como protocolo de encapsulamento, num contexto *web service*. Neste caso, deverá ainda prever-se a utilização de infraestruturas de acessos mediados (*web proxy*).

Regras de autenticação e Single Sign-On

O *Single Sign-On* (SSO) permite uniformizar a segurança dos mecanismos de autenticação e a consolidação das credenciais de autenticação e autorização utilizadas no Sistema de Informação. O SSO permite ainda aos utilizadores um ambiente aplicacional mais integrado, transparente e fluído e assim mais amigável na medida em que utilizam sempre as mesmas credenciais de autenticação e apenas uma única vez.

No caso de soluções com essa capacidade tecnológica, privilegia-se a utilização de autenticação recorrendo aos meios de integração OAuth 2.0 ou SAML suportados na Microsoft Azure Active Directory (Azure AD). Nos restantes casos, devem ser implementados os mecanismos *Single Sign-On* integrados no domínio Windows, assentes no protocolo *Kerberos*[1] e na infraestrutura LDAP over TLS da *Active Directory*[2]. Por integração entenda-se a utilização direta da *Active Directory* para fins de autenticação e autorização, respetivos repositórios de dados LDAP e todos os mecanismos inerentes *e.g.* protocolo de autenticação *Kerberos* (Kerberos v5), utilizando no contexto aplicacional Web o mecanismo (*pseudo security mechanism*) GSSAPI SPNEGO[3] (RFC 4178 – *Simple and Protected GSSAPI Negotiation Mechanism*).

A autenticação LDAP deve ser sempre efetuada utilizando LDAP over TLS ou LDAP over SASL[4] over GSSAPI/Kerberos e nunca LDAP em clear-text.

- Por omissão deverá ser implementado o mecanismo Single Sign-On (SSO) interativo para utilização em contextos em que o SSO automático não seja viável ou pretendido, *e.g.* o utilizador não se encontra autenticado no domínio ou não é possível a operação do mecanismo SPNEGO (Kerberos) com o cliente. Este deverá suportar-se num mecanismo de autenticação interativa Form-Based/Basic Authentication, utilizando-se as credenciais do utilizador do domínio Windows (Active Directory). Por forma a proteger as credenciais de domínio do utilizador (assim como de resto toda a informação tramitada na comunicação entre o cliente e o servidor), a solução deverá ser implementada em HTTP sobre o protocolo TLS (HTTPS) e LDAP sobre o protocolo TLS (LDAPS);
- Deverá implementar-se a possibilidade de SSO automático utilizando o pseudo-mecanismo de autenticação GSSAPI SPNEGO: Uma vez o utilizador autenticado no domínio Windows (*Active Directory*) não deverá ser solicitada novamente a autenticação para acesso ao sistema ou solução aplicacional considerados;
- Esta integração não deve suportar-se em repositórios réplicas e processos de sincronização da informação da AD.

[1] O Kerberos é um protocolo de autenticação segura através de um meio não seguro, desenhado originalmente no MIT. Assegura um método de autenticação robusto suportado em criptografia forte. O Kerberos realiza a autenticação como

um *trusted third-party authentication service*. Em termos gerais, o Kerberos oferece a autenticação mútua entre o cliente e o servidor. Utilizando criptografia simétrica (chave secreta) e assimétrica (chave pública), a troca de mensagens Kerberos está protegida contra interceção (*eavesdrop*). Um dos algoritmos de encriptação utilizados é o *Advanced Encryption Standard* (AES), dos mais avançados atualmente existentes. O protocolo Kerberos utiliza chaves de sessão (chaves de encriptação temporárias) e *tickets* (também com validade temporária) para assegurar a identidade das partes comunicantes. Esta infraestrutura é constituída por um componente central designado *Key Distribution Center* (KDC) que contém uma base de dados com as chaves secretas de cada um dos respetivos clientes e servidores e com eles individualmente partilhadas. Por sua vez este KDC consiste em dois componentes lógicos; um *Authentication Server* (AS) e um *Ticket Granting Server* (TGS). No processo de autenticação, o cliente, utilizando a sua chave secreta partilhada (e.g. password), a qual foi protegida por uma função criptográfica de *hash* (*one-way*, ou seja, irreversível), autentica-se apenas uma vez perante o AS do qual recebe um *ticket* (TGT - Ticket-Granting Ticket) e uma chave de sessão, ambos encriptados com a sua chave secreta partilhada. Utiliza de seguida este *ticket* e chave de sessão para se identificar perante o TGS para requisitar o acesso a um serviço. Se o cliente estiver autorizado para acesso ao serviço o TGS envia-lhe outro *ticket* (ST - Service Ticket) que o cliente utiliza para se apresentar junto do respetivo *Service Server* (SS).

[2] A *Active Directory* do domínio Windows é uma implementação LDAP (*Lightweight Directory Access Protocol*) da Microsoft utilizada como repositório de informação de domínio. O sistema operativo Windows e o respetivo repositório *Active Directory* (AD), utilizado para autenticação e autorização no domínio Windows, suportam-se no protocolo Kerberos como método de autenticação nativo (Kerberos v5).

[3] O GSSAPI (*Generic Security Services Application Programming Interface*) é uma API genérica de autenticação, sendo o SPNEGO (*Simple and Protected GSS-API Negotiation Mechanism*) um pseudo-mecanismo de autenticação utilizado neste contexto em HTTP para negociação de um mecanismo de autenticação, normalmente Kerberos.

[4] O SASL (*Simple Authentiction and Security Layer*) é um network protocol para autenticação client-server disponibilizando uma forma de negociação do método de autenticação a utilizar e da sua realização. Um plugin SASL comum é o GSSAPI normalmente utilizado com Kerberos.

Conformidade com a Política de Utilização de Normas Abertas

Com a utilização de software proprietário existe o risco efetivo de se ficar reféns de soluções tecnológicas específicas que utilizam especificações proprietárias (fechadas) de formatos e protocolos, muitas vezes suportadas por práticas monopolistas anticoncorrenciais, cujo objetivo não é de todo favorecer o utilizador. Estas especificações proprietárias, por vezes designadas como *standards*, apenas estão disponíveis sob termos contratuais restritivos estabelecidos pelas entidades proprietárias da especificação, condicionando fortemente a interoperabilidade entre os sistemas. A hegemonia que certas soluções proprietárias criaram, também acarreta outras consequências mais subtis, ao abrirem caminho a certas derivas lesivas para a liberdade e privacidade dos cidadãos.

Tendo como objetivo a interoperabilidade entre diferentes soluções, sistemas, plataformas e aplicações, um standard aberto (norma ou padrão aberto) é uma especificação (e.g. de formatos abertos, protocolos abertos) que resulta de um processo no qual participam todas as partes interessadas e se encontra publicamente disponível com direitos de utilização associados que garantam sem restrições de qualquer espécie, critérios de livre acesso, implementação, utilização, transparência e imparcialidade:

- As especificações devem estar publicamente disponíveis e acessíveis para consulta, implementação, desenvolvimento, utilização, cópia e distribuição sem restrições e livres de *royalties* (*royalty-free*) ou outras taxas.
- As normas abertas não podem assumir qualquer carácter discriminatório nem permitir dar existência a implementações que o tenham.
- As patentes ou outros direitos de Propriedade Intelectual eventualmente presentes numa norma aberta devem ser disponibilizadas livre de *royalties* (*royalty-free*) sob termos de licenciamento irrevogáveis e irreversíveis.

O termo norma aberta encontra-se muito associado ao software livre na medida em que se considera que uma norma não é aberta se não permitir uma implementação plena em software livre. Porque o software livre utiliza normas de protocolos e formatos abertos e livres, existe um total conhecimento dos formatos dos dados, dos protocolos e a forma como estão implementados. Fica assim assegurada a compatibilidade, a interoperabilidade e a comunicação transparente, mesmo entre sistemas diferentes.

Conforme decorre da legislação nacional, Lei n.º 36/2011 de 21 de junho que "*Estabelece a adoção de normas abertas nos sistemas informáticos do Estado*" e do "*Regulamento Nacional de Interoperabilidade Digital (RNID)*" publicado na Resolução do Conselho de Ministros n.º 2/2018, o desenvolvimento ou a implementação de soluções tecnológicas deverá ser conformidade as convenções, protocolos e formatos especificados sob a definição de normas abertas. Esta regra aplica-se também aos formatos dos documentos eletrónicos disponibilizados ao utilizador por qualquer via que devem encontrar-se em formatos que todos possam utilizar, e não apenas nos formatos proprietários ou que exijam a utilização de software proprietário.

Normas abertas (formatos e protocolos abertos)

Alguns dos standards que têm de ser seguidos no âmbito do desenvolvimento ou implementação de soluções de software (quando aplicáveis ao contexto em causa), são os da família de standards IETF onde se incluem os standards Internet Request for Comments (RFC), os da família de standards ISO/IEC, dos standards IEEE onde se incluem os standards IEEE 802 (LAN, MAN) e os standards IEEE 1003 (POSIX), dos standards ITU (e.g. G, H, T, X, V) e os da família de standards W3C, entre outros.

Conformidade com a Política de Utilização de Software Livre

Em setembro de 2004 foi aprovada a Resolução da Assembleia da República n.º 66/2004, que recomenda ao Governo a tomada de medidas com vista ao desenvolvimento do software livre em Portugal, entre elas a implementação de soluções de software livre na Administração Pública e a integração do software livre nas soluções existentes.

O software livre, conforme definido pela *Free Software Foundation* (FSF), é todo o software que pode ser utilizado, copiado, estudado, modificado e redistribuído sem restrições. As quatro liberdades em que assenta o software livre, são:

- A liberdade para se utilizar o software, para qualquer propósito (*freedom* 0)
- A liberdade para estudar o funcionamento do software e adaptá-lo às necessidades (*freedom* 1). *O acesso ao código fonte (source code) é uma pré-condição para esta liberdade.*
- A liberdade para redistribuir cópias desse software (*freedom* 2)
- A liberdade para melhorar o software, e disponibilizar essas modificações publicamente por forma que toda a comunidade beneficie (*freedom* 3). *O acesso ao código fonte é uma pré-condição para esta liberdade.*

Sendo a libertação de restrições o conceito fulcral, todo o software que observar os quatro princípios ou liberdades do FSF é designado "software livre" (*free software*).

O oposto do software livre é o software proprietário. No entanto, deve-se ter presente que esta distinção não tem qualquer relação com o custo ou gratuitidade do software. Esta é aliás uma confusão usual quando se aborda a definição de software livre (*free software*) com origem na ambiguidade do termo inglês *free* que tem ambos significados, grátis ou livre. O erro está em entender-se *free* como grátis, *i.e.* algo não comercial. Desta forma, surge o entendimento incorreto de que o software livre não é comercial, fazendo-se a associação desta noção apenas ao software proprietário. Contudo, a utilização do termo *free* em *free software* significa livre, e não grátis, podendo o software livre ser também comercializado. Aliás, qualquer restrição à comercialização ou imposição de gratuitidade do software livre resultaria numa clara contradição com as liberdades definidas.

Da mesma forma também a ideia de que o software proprietário é sempre comercial está errada. Tal como o software livre, também o software proprietário pode ser ou não comercial. Ser proprietário não implica ser comercial, tal como reciprocamente ser comercial não implica ser proprietário. Por exemplo, o *freeware* é software proprietário. Este software pode ser distribuído com algumas ou nenhuma das liberdades anteriormente enunciadas, apresentando-se normalmente com uma licença *End-User License Agreement* (EULA). Contudo, o *freeware* é gratuito, *i.e.* não comercial. A gratuitidade não garante, nem na realidade tem alguma relação com as liberdades do software livre.

O aspeto comercial não distingue o software livre do software proprietário, pois ambos os modelos podem assumir igualmente essa condição. Apenas a garantia das liberdades enunciadas fazem a distinção.

As duas maiores categorias de licenças de software livre, são as licenças *copyleft* e *non-copyleft*. As licenças *copyleft*, como a GNU GPL, insistem em que as versões modificadas de um software livre, têm de permanecer da mesma forma como software livre. As licenças *non-copyleft*, como as licenças BSD, não insistem nisto, permitindo mesmo que o software, nas suas versões modificadas ou originais, deixe de ser livre, *i.e.* passem a ser software proprietário.

Embora as licenças *copyleft* sejam as recomendadas, na medida em que protegem a liberdade para todos os utilizadores, o software que utiliza as licenças *non-copyleft*, pode mesmo assim ser software livre, e útil para a comunidade.

Globalmente, os tipos de licenças de software livre atualmente existentes são os seguintes:

- Licenças *copyleft*, como a GNU General Public License, a mais proeminente - o autor retém o copyright e utiliza-o para permitir a modificação e redistribuição sob termos que assegurem que todas as versões modificadas permaneçam livres;

- Licenças do tipo BSD (*non-copyleft*), assim designadas porque se aplicam à maioria do software distribuído nos sistemas operativos BSD - o autor retém os direitos de cópia, apenas para impor a apresentação do aviso do copyright, fazendo a referência ao autor original do trabalho, nas versões modificadas ou derivadas. Permite a redistribuição e modificação e mesmo a utilização em software proprietário, pois não obriga que as versões modificadas ou derivadas permaneçam livres;

- Domínio público - o domínio público não é uma licença, mas um estado. Significa que o material, software ou outro, não está protegido por copyright, não sendo assim necessária uma licença. Uma vez que o software em domínio público não tem a proteção do copyright, pode ser livremente incorporado em qualquer trabalho quer seja software proprietário ou livre. Como o autor abdica do copyright, não existe nenhum tipo de restrição sobre o software que fica assim completamente fora do seu controlo e, mesmo querendo, não pode mais tarde impor qualquer restrição.

A maior parte do software livre, utiliza um pequeno conjunto de licenças, entre as quais as mais populares são a GNU General Public License (GPL), a GNU Lesser General Public License (LGPL), a Modified BSD License, a Mozilla Public License, a MIT License, e a Apache License.

No desenvolvimento de software à medida para a ANACOM serão rejeitadas quaisquer propostas de restrição ou reserva dos direitos de utilização do software e materiais conexos, do respetivo código fonte, da propriedade intelectual (ideias, métodos, técnicas, algoritmos, patentes, especificações), da revelação de qualquer informação inerente, ou outras que inviabilizem ou limitem de qualquer forma, no todo ou em parte, ou em qualquer momento que o licenciamento do software desenvolvido se possa fazer como software livre. Para qualquer efeito deve este software, e respetivo código fonte, ser considerado propriedade total da ANACOM, podendo este dele dispor conforme entender e inclusive, no âmbito das suas atribuições de

promoção do desenvolvimento do acesso à sociedade de informação e do conhecimento, partilhá-lo com outros organismos do Estado ou até disponibilizá-lo à sociedade como Software Livre. Quaisquer direitos de propriedade intelectual ou de utilização eventualmente presentes no software desenvolvido à medida devem ser disponibilizados sob termos de licenciamento irrevogáveis e irreversíveis à ANACOM que deterá todos os direitos de utilização, incluindo a alteração, melhoramento e redistribuição do software para qualquer propósito.

Regras de utilização de software third-party

A introdução de código que não faça parte da infraestrutura existente na ANACOM e que não seja da autoria ou propriedade do fornecedor do projeto em desenvolvimento ou de implementação da solução de software, aqui designados de componentes de *software* aplicacionais *third-party* (*e.g.* bibliotecas de classes Java), tem de ser previamente aprovada pela ANACOM a fim de não ocorrer qualquer utilização ilegal, por violação dos termos da licença do software, assim como situações de risco de segurança decorrentes da utilização de software a partir de fontes desconhecidas ou não confiáveis.

Assim, deverão ser sempre previamente explicitados pelo fornecedor, em formato matricial, todos os aspetos relacionados com o código ou solução em causa, assim como o seu enquadramento no projeto, a sua origem, *copyright* e licença de utilização (*e.g.* GNU GPL, LGPL, BSD, MIT, ISC, ASL, MPL), que naturalmente não podem colidir com direitos de terceiros. O fornecedor aguardará pela aprovação da ANACOM antes de introduzir estes componentes no desenvolvimento ou implementação da solução. Apenas serão aceites aqueles cuja licença o defina como software livre *e.g.* licenças *copyleft* como a GNU GPL/LGPL ou compatíveis.

Conformidade com a Legislação Nacional sobre a Assinatura digital

Em conformidade com a legislação nacional vigente, a aposição a um documento eletrónico de uma assinatura digital qualificada certificada por entidade certificadora credenciada, equivale à assinatura autografa desse documento e garante o não-repúdio. Para efeitos de assinatura digital qualificada com o valor probatório pleno que lhe é reconhecido, é necessário um Certificado Digital Qualificado emitido por uma entidade certificadora credenciada - Decreto-Lei n.º 88/2009 de 9 de abril.

Assim, e em conformidade com a legislação, a chave privada de assinatura digital, correspondente à chave pública de verificação, apenas pode encontrar-se sob controlo do respetivo titular, em *tokens*, *SmartCards* ou outros dispositivos criptográficos adequados ao seu armazenamento.

Sempre que definidos requisitos funcionais quanto à qualidade do valor probatório dos documentos eletrónicos no âmbito jurídico, terá de ser utilizada a assinatura digital qualificada, recorrendo a certificados digitais qualificados PKI ITU-X.509 emitidos por Entidade Certificadora (EC) credenciada pela Autoridade Credenciadora (AC).

Caso se pretenda a *notarização* eletrónica (desmaterialização do processo de reconhecimento notarial de assinaturas), é necessário além do não repúdio (assinatura digital) a implementação de mecanismos de validação dos objetos assinados digitalmente com recurso ao *time-stamping*.

Legislação aplicável: Decreto-Lei n.º 88/2009, de 9 de abril - Assinatura eletrónica: Alteração ao Decreto-Lei n.º 290-D/99, de 2 de agosto (Alteração dos artigos 5.º, 28.º, 29.º, 38.º e 40.º do Decreto-Lei n.º 290-D/99, de 2 de Agosto, alterado pelos Decretos-Leis n.ºs 62/2003, de 3 de Abril, 165/2004, de 7 de Junho, e 116-A/2006, de 16 de Junho).

Time-Stamp Protocol

O *Time-Stamp Protocol* (IETF RFC 3161 - TSP) utiliza o conceito de um fornecedor de serviço confiável. Considerando o protocolo como um tipo de serviço, existem três partes: *a*) aqueles que consideram o *time-stamp* gerado uma prova de que determinada peça de informação existia num determinado momento; *b*) o assinante, que é o utilizador de *time-stamp*; *c*) a *Time-Stamping Authority* (TSA), que é o fornecedor de serviço e que, entre outros requisitos, utiliza uma fonte de tempo legal.

Seguindo o protocolo TSP, o utilizador do serviço envia uma requisição com o *hash* do documento (do qual pretende a certificação temporal) num formato bem definido para o fornecedor (TSA). Este devolve uma resposta digitalmente assinada contendo o *hash* do documento e o *time-stamp* (data/hora). Esta especificação (RFC 3161) define as mensagens (requisição e resposta) e estruturas de dados utilizadas no protocolo e descreve a sua utilização sobre protocolos de transporte, *e.g. sockets* TCP, ou encapsulado em HTTP, FTP, SMTP (IETF RFC 3161 - *Part 3. Transports*).

Os protocolos de transporte devem apenas implementar o padrão requisição-resposta, cada qual com requisitos próprios: *e.g.* as requisições HTTP, devem ter o "Content-Type" definido como

"application/timestamp-query", enquanto a resposta deve ter esse atributo definido como "application/timestamp-reply". Assim, quando um assinante envia uma requisição via FTP ou HTTP, a ligação com o fornecedor deve permanecer ativa até que seja devolvida uma resposta. Como os recursos de rede nem sempre são abundantes, ambas as partes do protocolo sofrem com a manutenção da ligação, principalmente o servidor. A especificação do TSP via *sockets* contorna esse problema, recorrendo ao conceito de *polling*, que passa por efetuar requisições periódicas, em intervalos de tempo definidos pelo servidor.

Utilização do Serviço de Correio Eletrónico

Caso seja necessário o envio ou receção de correio eletrónico no âmbito da solução de software a desenvolver ou implementar, deverão ser observadas as seguintes regras:

- O envio de email é efetuado utilizando o protocolo SMTP, respeitando as normas IETF RFC 5321, 5322, 3207, 8314, 3461, 3463, 3464, 3798, 3886, 1421, 2045, 2046, 2047, 2183, 2231, 6376, 7208, 7489, 8617 e conexos. Para esse efeito, existe uma infraestrutura servidora de correio eletrónico on-premises hibridizada com uma infraestrutura de correio eletrónico na cloud, podendo ambas ser utilizadas no mesmo contexto de email do domain anacom.pt dependendo apenas de a solução se encontrar on-premises ou na cloud;

- A receção de email é efetuada em *mailbox* própria criada para utilização da solução em causa. As mensagens de correio eletrónico recebidas nesta *mailbox* podem ser integradas na solução através da utilização do protocolo IMAP4 (IETF RFC 3501). Para esse efeito existe igualmente uma infraestrutura servidora de correio eletrónico on-premises hibridizada com uma infraestrutura de correio eletrónico na cloud, podendo ambas ser utilizadas no mesmo contexto de email do domain anacom.pt dependendo apenas de a solução se encontrar on-premises ou na cloud;

- O envio de mensagens de correio eletrónico (email) deve ser efetuado utilizando endereços remetentes existentes previamente criados para utilização específica da solução em causa. Esses endereços deverão estar associados a *mailboxes* internas da ANACOM já existentes. Caso se pretenda que as respostas sejam encaminhadas para endereços diferentes do endereço remetente, deverá ser utilizado o ***header*** "*Reply-To*". Caso se pretenda enviar mensagens de correio eletrónico (email) com origem num endereço mas em nome de outro, deverá ser utilizado no ***from*** do envelope da mensagem (RFC5321.MailFrom) e no ***header*** "Sender" (RFC5322.Sender) o endereço de facto remetente da mensagem, com a colocação concomitante do endereço em nome do qual se pretende enviar a mensagem no ***header*** "From" (RFC5322.From). Contudo, a fim de evitar dificuldades (*e.g.* com validações), esta prática deverá ser evitada;

- O envio de email deve ser efetuado a partir da plataforma aplicacional de suporte à solução e não da plataforma de base de dados ou outra;

- O interface de email da aplicação, ficará sujeito à política global e termos de utilização do serviço de correio eletrónico global, *i.e.* filtros anti-malware, anti-phishing, anti-spam, limites e volumetrias estabelecidas, políticas de autenticação e autorização SPF (IETF RFC 7208), DKIM (IETF RFC 6376) e DMARC (IETF RFC 7489).

Regras de comunicação eletrónica

Por forma a assegurar confidencialidade, a integridade e a autenticidade da informação tramitada por via eletrónica (*e.g.* email, web), deverão ser utilizados meios criptográficos. Os mecanismos adequados para

cumprir este requisito, passam pela utilização de criptografia assimétrica (chave pública/privada) para encriptação e assinatura digital.

Esta regra aplica-se também a toda a documentação e conteúdos tramitados com a ANACOM, por meios de comunicação eletrónica, durante o desenvolvimento ou manutenção do software. Os dados e informação a proteger, podem ser quaisquer conteúdos aplicacionais, código-fonte, objetos compilados, executáveis, bibliotecas de funções ou classes, configurações, *scripts* SQL DDL/DML, bases-de-dados, ou *packages* contendo estes conteúdos, *exports*, *backups*, documentos de informação técnica, especificações ou requisitos, de infraestruturas, de sistemas, interfaces (APIs), esquemas e diagramas UML, E/A ou relacionais ou descrição das estruturas de tabelas de base de dados.

Podem utilizar-se implementações dos modelos PGP (*Web-of-Trust*) ou PKI (*Chain-of-Trust*) com certificados digitais ITU X.509v3.

Por omissão, a infraestrutura de correio eletrónico da ANACOM utiliza sempre o protocolo TLS nas comunicações SMTP tanto no envio como na receção, nos mesmos termos anteriormente indicados relativamente às comunicações HTTP.