ÁGUAS DO NORTE, S.A.

CONCURSO PÚBLICO

PRC_0225/2020_STI – Aquisição de serviços de Cibersegurança para a Águas do Norte, S.A.

CADERNO DE ENCARGOS

CARLA ISABEL OLIVEIRA NUNES

Assinado de forma digital por CARLA ISABEL OLIVEIRA NUNES
Dados: 2020.09.08 17:12:10 +01'00'

CAPÍTULO I
DISPOSIÇÕES GERAIS

Cláusula 1.ª
Objeto

1. 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 de serviços de Cibersegurança para a Águas do Norte, S.A., em conformidade com a norma ISSO/IEC27001 e com as observâncias constantes no Anexo I do presente Caderno de Encargos.

2. O objeto do presente contrato compreende os seguintes serviços:

   - Serviços de Centro de Operações de Segurança;
   - Serviços de CIBERSEGURANÇA;
   - Serviços de AUDITORIA, COMPLIANCE, CIBERSEGURANÇA da Águas do Norte, S.A. para a certificação ISO/IEC27001.

Cláusula 2.ª
Elementos do 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 pelo concorrente, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
   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 divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.

4. Em caso de divergência 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 e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma legal.
5. O estabelecimento, na proposta, de termos ou condições não admitidas por este caderno de encargos e que não tenham sido detetados em fase pré-contratual consideram-se, para efeitos de execução do contrato, como não escritos e de nenhum efeito.

Cláusula 3.ª
Preço Base

1. O preço base do procedimento é, nos termos e para os efeitos do disposto no artigo 47.º do Código dos Contratos Públicos, de 136.000,00 EUR (cento e trinta e seis mil euros), não incluindo o Imposto Sobre o Valor Acrescentado, para o período de execução contratual de 3 (três) anos.

2. Não obstante o referido no número anterior, são ainda fixados preços base unitários, de acordo com o definido no Anexo IV do Programa do Procedimento.

Cláusula 4.ª
Vigência

1. O contrato a celebrar terá a duração de 3 (três) anos, a contar da data da respetiva outorga, cessando o contrato no final desse período ou no momento em que a AdNorte, tenha pago ao Adjudicatário o preço estimado da proposta que vier a ser adjudicada.

CAPÍTULO II
OBRIGAÇÕES DAS PARTES

SECÇÃO I
OBRIGAÇÕES DO ADJUDICATÁRIO

Cláusula 5.ª
Obrigações do adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável e no presente Caderno de Encargos, constituem obrigações principais do adjudicatário as seguintes:

a) Obrigação de execução dos serviços identificados na sua proposta;

b) Disponibilizar o número suficiente de técnicos com qualificação técnico-científica adequada, de forma a garantir uma eficiente concretização dos objetivos definidos no presente Caderno de Encargos, além de uma correta articulação entre o prestador de serviços e os representantes da Águas do Norte, S.A.;

c) Designar um responsável pela prestação de "Serviços de Cibersegurança";

d) Executar os "Serviços de Cibersegurança" que lhe for adjudicado, tal como descrito no presente Caderno de Encargos, com absoluta subordinação aos princípios da ética profissional, isenção, independência, zelo e competência;

e) Cumprir as condições fixadas para a execução dos "Serviços de Cibersegurança";

f) Sujeitar-se à ação fiscalizadora da Águas do Norte, S.A.;

g) Garantir o sigilo quanto à informação a que o pessoal envolvido nos trabalhos venha a ter acesso;

h) Prestar as informações que forem solicitadas pela Águas do Norte, S.A.;

i) Realizar todos os trabalhos previstos no Caderno de Encargos, nas condições de prazo e preço contratados;

j) A comunicação à Águas do Norte, S.A., logo que tenha conhecimento, dos factos que tornem total ou parcialmente impossível a execução do contrato ou a deteção de eventuais falhas que alterem a qualidade da prestação do serviço conforme especificado;

k) A informação, de forma correta e fidedigna, referente às condições em que se processa a execução contratual, bem como a prestação de todos os esclarecimentos solicitados pela Águas do Norte, S.A., designadamente pelo gestor de contrato que esta designar;

l) Comunicação de qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação social ou os seus representantes legais;

2. A título acessório, o adjudicatário fica também obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação do serviço, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

3. O adjudicatário é ainda responsável perante a AdNorte por qualquer defeito ou discrepância dos recursos materiais e informáticos afetos à prestação dos "Serviços de Cibersegurança"

4. O Adjudicatário obriga-se a cumprir a legislação em vigor em matéria de proteção jurídica dos programas de computador, nomeadamente o DL n.º 252/94, de 20 de Outubro, na sua atual redação, o Código do Direito de Autor e dos Direitos Conexos, aprovado pelo DL n.º 63/85, de 14 de Março, na sua atual redação e o Código da Propriedade Industrial, aprovado pelo DL n.º 36/2003, de 05 de Março, na sua atual redação.

5. O Adjudicatário obriga-se ainda a observar o estabelecido em matéria de proteção de dados pessoais, nomeadamente com as orientações e determinações emanadas pelo Regulamento (EU) 2016/679, de 27 de abril de 2016 e demais normativos conexos.

Subsecção I
Âmbito dos serviços a fornecer.

Cláusula 6.ª
Componente de assistência técnica e manutenção evolutiva

1. Os serviços relacionados com as componentes de assistência técnica e de manutenção evolutiva da solução serão prestados tendo como âmbito as instalações administrativas, técnicas e operacionais da Águas do Norte, S.A. que constituem o Sistema Multimunicipal de Abastecimento de Água e Saneamento da Águas do Norte e serão executados na Sede localizada em Vila Real e na ETA de Areias de Vilar localizada em Barcelos.
2. A prestação dos serviços devem ser prestados conforme descrito no Anexo I do presente Caderno de Encargos.
3. Os serviços de suporte técnico especializado serão objeto de prévia solicitação pela Águas do Norte, S.A. ou por sua prévia aprovação, neste último caso, se a iniciativa pertencer ao adjudicatário.
4. O suporte técnico especializado será prestado *in situ* nos locais indicados no número 1 da presente cláusula;

5. As intervenções técnicas especializadas serão solicitadas, no helpdesk da Águas do Norte, S.A.(SICO), originando o pedido de incidente, projeto ou de serviço, comunicado via correio eletrónico.
6. Relativamente às mesmas componentes, quaisquer serviços não previstos só serão realizados por solicitação expressa da Águas do Norte, S.A., ou por proposta do adjudicatário, mediante acordo prévio da Águas do Norte, S.A., sendo sempre efetuados dentro das condições aqui definidas, ou outras que venham a ser para o efeito acordadas.

Cláusula 10.ª
Direitos de propriedade intelectual e industrial

1. O adjudicatário terá que demonstrar ser titular de todas as licenças, autorizações ou demais atos de consentimento legalmente necessários à utilização de *software* e demais soluções ou produtos por si utilizados na execução do contrato a celebrar.

2. O adjudicatário obriga-se a manter válidas as licenças, autorizações ou demais atos de consentimento a que se refere o número anterior, até à integral execução dos serviços contratados.

Cláusula 11.ª
Transferência da propriedade

1. Os elementos apresentados pelo adjudicatário ao abrigo do contrato passam a integrar a propriedade da Águas do Norte, S.A., incluindo os direitos autorais sobre todas 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.

Cláusula 12.ª
Conformidade e garantia técnica

O adjudicatário fica sujeito, com as devidas adaptações e no que se refere aos elementos entregues à Águas do Norte, S.A. em execução do contrato, às exigências legais, às obrigações do fornecedor e prazos respetivos aplicáveis aos contratos de aquisição de serviços, nos termos do Código dos Contratos Públicos e demais legislação aplicável.

SUBSECÇÃO I
DEVER DE SIGILO

Cláusula 13.ª
Objeto do dever de sigilo

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à Águas do Norte, S.A., de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.

2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.

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

Cláusula 14.ª
Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor até ao termo do prazo de 2 (*dois*) anos 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.

Cláusula 15.ª
Proteção de dados pessoais e RGPDR

1. O adjudicatário obriga-se, durante a vigência do contrato e mesmo após a sua cessação, a não ceder, revelar, utilizar ou discutir, com quaisquer terceiros, todas e quaisquer

informações e ou elementos que lhe hajam sido confiados pela Águas do Norte, S.A. ou de que tenha tido conhecimento no âmbito do contrato ou por causa dele.

2. Os dados pessoais a que o prestador de serviços tenha acesso ou que lhe sejam transmitidos pela Águas do Norte, S.A. ao abrigo do contrato serão tratados em estrita observância das instruções desta empresa e da legislação de Proteção de Dados Pessoais, nomeadamente com o Regulamento Geral de Proteção de Dados Pessoais (RGPD - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016)
3. O prestador de serviços compromete-se, designadamente, a não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou por qualquer outra forma colocar à disposição de terceiros os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pela Águas do Norte, S.A. ao abrigo do contrato, sem que para tal tenha sido expressamente instruída, por escrito, pela Águas do Norte, S.A..
4. O prestador de serviços aceita que a Águas do Norte, S.A. recorra a outras entidades subcontratadas exclusivamente com o intuito de prestar serviços a que o prestador de serviços não consiga dar resposta, sempre no âmbito das atribuições definidas pela Águas do Norte, S.A.
5. Caso o prestador de serviços subcontrate outras entidades (mediante prévia autorização escrita da Águas do Norte, S.A., nos termos previstos no CCP) para a prestação de serviços previamente definidos pela Águas do Norte, S.A., o prestador de serviços será o único responsável pela escolha das empresas subcontratadas, bem como por toda a atuação destas.
6. O prestador de serviços obriga-se a garantir que as empresas por esta subcontratadas cumprirão o disposto na LPDP e na demais legislação aplicável, nomeadamente com o Regulamento Geral de Proteção de Dados Pessoais (RGPD - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016), devendo tal obrigação constar dos contratos escritos que a celebra com outras entidades por si subcontratadas.
7. O prestador de serviços obriga-se a cumprir rigorosamente o disposto na LPDP e demais legislação aplicável em matéria de tratamento de dados pessoais e nomeadamente a:

a) Utilizar os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pela **Águas do Norte, S.A.**, única e exclusivamente para efeitos da prestação dos serviços objeto deste contrato;

b) Observar os termos e condições constantes dos instrumentos de legalização respeitantes aos dados tratados;

c) Manter os dados pessoais estritamente confidenciais, cumprindo e garantindo o cumprimento do dever de sigilo profissional relativamente aos mesmos dados pessoais;

d) Cumprir quaisquer regras relacionadas com o tratamento de dados pessoais a que a **Águas do Norte, S.A.**, esteja especialmente vinculada, desde que tais regras lhe sejam previamente comunicadas;

e) Pôr em prática as medidas técnicas e de organização necessárias à proteção dos dados pessoais tratados por conta da **Águas do Norte, S.A.**, contra a respetiva destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais;

f) Prestar à **Águas do Norte, S.A.**, toda a colaboração de que esta careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais efetuado ao abrigo do contrato e manter a **Águas do Norte, S.A.**, informada em relação ao tratamento de dados pessoais, obrigando-se a comunicar de imediato qualquer situação que possa afetar o tratamento dos dados em causa ou que de algum modo possa dar origem ao incumprimento das disposições legais em matéria de proteção de dados pessoais ou dos termos do instrumento de legalização concedido pela Comissão Nacional de Proteção de Dados à **Águas do Norte, S.A.**, EPAL;

g) Assegurar que os seus colaboradores cumprem todas as obrigações previstas no contrato;

i) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

j) Adotar medidas de segurança previstas no artigo 32.° do RGPD, que assegurem a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços que tratam dados pessoais e possuir um processo para testar, apreciar e avaliar regularmente a eficácia destas medidas;

k) Prestar a assistência necessária à **Águas do Norte, S.A.** no sentido de permitir que esta cumpra a obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos Direitos previstos no RGPD, nomeadamente o direito de acesso do titular aos seus dados pessoais, direito de retificação e direito ao apagamento dos dados.

l) Garantir mecanismos de notificação efetivos em caso de violação de dados pessoais;

m) Disponibilizar as informações necessárias para demonstrar o cumprimento do RGP, bem como colaborar com auditorias ou inspeções, conduzidas pela **Águas do Norte, S.A.** ou por outro auditor por este mandatado.

8. O prestador de serviços será responsável por qualquer prejuízo em que a **Águas do Norte, S.A.**, venha a incorrer em consequência do tratamento, por parte do mesmo e/ou dos seus colaboradores, de dados pessoais em violação das normas legais aplicáveis e/ou do disposto no contrato.

9. Para efeitos do disposto no n.º 8 e na alínea g) do n.º 7 da presente cláusula, entende-se por "colaborador" toda e qualquer pessoa singular ou coletiva que preste serviços ao adjudicatário/prestador de serviços, incluindo, designadamente, representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido entre o adjudicatário e o referido colaborador.

10. A obrigação de sigilo prevista na alínea d) do número 7 da presente cláusula mantém-se mesmo após a cessação do contrato, independentemente do motivo porque ocorra.

Cláusula 16.ª

Inoperabilidade digital

O adjudicatário obriga-se a executar o contrato em conformidade com as normas abertas:

i. Lei n.º 36/2011, de 21 de junho - Adoção de normas abertas nos sistemas informáticos do Estado
ii. RCM n.º 91/2012, de 8 de novembro - Regulamento Nacional de Interoperabilidade Digital

SECÇÃO II
OBRIGAÇÕES DA ADNORTE

Cláusula 17.ª

Preço contratual

1. Pela prestação de serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a Águas do Norte, S.A. deve pagar ao adjudicatário os preços unitários constantes da proposta, acrescido de IVA à taxa legal em vigor, se este for legalmente devido, sem prejuízo do disposto no número seguinte.
2. O preço total é estimado, por ser variável em função das quantidades de serviços efetivamente realizados, razão pela qual a Águas do Norte, S.A. apenas pagará os serviços que venham a ser real e efetivamente prestados, por aplicação dos preços unitários previstos para os tipos de trabalho indicados às intervenções efetivamente realizadas.
3. As quantidades apresentadas no presente de Caderno de Encargos são meramente indicativas, destinando-se, essencialmente, à determinação do preço total estimado.
4. Caso venha a verificar-se que o valor dos serviços efetivamente prestados é menor do que o valor correspondente às quantidades estimadas apresentadas nas Cláusulas deste

Caderno Encargos, o adjudicatário não terá direito a qualquer indemnização ou compensação, sem prejuízo do disposto no n.º 1 do artigo 381.º, aplicável de acordo com n.º 6 do artigo 454.º, ambos do CCP.

5. O preço referido nos números anteriores inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à Águas do Norte, S.A., nomeadamente os relativos aos meios humanos e materiais, alimentação, transporte, armazenamento e manutenção, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.
6. Não haverá lugar à revisão de preços durante o prazo de execução contratual e eventuais renovações se as houver.

Cláusula 18.ª

Condições de pagamento

1. As quantias devidas pela Águas do Norte, S.A., nos termos da(s) cláusula(s) anterior(es), deve(m) ser paga(s) no prazo de 30 (*trinta*) dias após a receção pela Águas do Norte, S.A. das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.

2. As faturas a apresentar pelo Adjudicatário à Águas do Norte, S.A., devem conter os elementos necessários a uma completa, clara e adequada compreensão dos valores faturados, os quais devem ser apresentados de forma desagregada em documento anexo a cada fatura. Em caso de discordância por parte da Águas do Norte, S.A. quanto aos valores indicados nas faturas, deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

3. Desde que devidamente emitidas e observado o disposto nos pontos anteriores, da presente Cláusula, as faturas devem ser apresentadas até ao dia 4 do mês seguinte a que se referem, conter a menção da respetiva nota de encomenda e são pagas através de transferência bancária.

Cláusula 19.ª

Erros e omissões do caderno de encargos

1. O Adjudicatário deve, no prazo de 60 dias contados da data da celebração do contrato, reclamar sobre a existência de erros ou omissões do caderno de encargos, salvo dos que só sejam detetáveis durante a execução do contrato, sob pena de ser responsável por suportar metade do valor dos trabalhos complementares de suprimento desses erros e omissões.
2. O Adjudicatário é ainda responsável pelos trabalhos complementares que se destinem ao suprimento de erros e omissões que, não podendo objetivamente ser detetados na fase de formação do contrato, também não tenham sido por ele identificados no prazo de 30 dias a contar da data em que lhe fosse exigível a sua deteção.
3. Sem prejuízo do disposto nos números anteriores, caso os erros ou omissões decorram do incumprimento de obrigações de conceção assumidas por terceiros perante a Águas do Norte, S.A.:
    a) Deve a Águas do Norte, S.A. exercer obrigatoriamente o direito que lhe assista de ser indemnizado por parte destes terceiros;
    b) Fica o Adjudicatário sub-rogado no direito de indemnização que assiste à Águas do Norte, S.A. perante esses terceiros até ao limite do montante que deva ser por si suportado em virtude do disposto dos n.ºs 1 e 2 da presente Cláusula.

Cláusula 20.ª

Acompanhamento e controlo do contrato

1. Para o acompanhamento da execução do contrato, a Águas do Norte, S.A. poderá requerer ao Adjudicatário reuniões de acompanhamento à execução do contrato.
2. Todos os relatórios, registos, comunicações, e demais documentos elaborados pelo Adjudicatário devem ser integralmente redigidos em português.
3. O adjudicatário obriga-se a dispor de um responsável pela execução do contrato.
4. Após a assinatura do contrato, o adjudicatário informará, por escrito, o nome do responsável, indicando a sua qualificação técnica e, ainda, se o mesmo pertence ou não ao seu quadro técnico legal.
5. As ordens, avisos e notificações que se relacionem com os aspetos técnicos da execução dos serviços poderão ser dirigidos diretamente ao seu responsável.
6. O adjudicatário deverá assegurar os meios indispensáveis para o estabelecimento de uma comunicação eficaz entre os seus agentes através da atribuição de um telemóvel, facultando o respetivo número à Águas do Norte, S.A.

7. Em complemento dos meios de comunicação móveis, deverá ainda dispor de ligação à rede fixa com os meios indispensáveis para o estabelecimento de comunicação compatível entre a Águas do Norte, S.A. e o adjudicatário. É igualmente obrigatório dispor de meios que permitam a comunicação por correio eletrónico.

Cláusula 21.ª

Seguros e Encargos Sociais

1. Seguro de Responsabilidade Civil

a) O adjudicatário subscreverá em seu próprio nome e de todos os eventuais contratados e trabalhadores independentes, uma apólice de seguro onde serão indemnizadas, em caso de sinistro, as perdas e/ou danos de caráter patrimonial e não patrimonial, causados a terceiros em geral e à Águas do Norte, S.A. em particular, em consequência da execução da presente prestação de serviços, cuja responsabilidade civil legal de natureza extracontratual pelo dano causado seja imputável a qualquer das entidades seguras na apólice, por si isoladamente ou de forma solidária;

b) Para todos os efeitos deste seguro, deverá constar nas Condições Particulares da Apólice que a entidade adjudicante será sempre considerada terceira, independentemente da sua relação jurídica com o tomador do seguro;

c) O Adjudicatário é obrigado a contratar um seguro de responsabilidade civil que garanta a cobertura dos riscos e danos direta ou indiretamente emergentes da sua atuação no valor mínimo de 150.000,00 EUR (cento e cinquenta mil euros) por sinistro e anuidade.

2. Seguro de Acidentes de Trabalho

a) O Adjudicatário ficará responsável pelo pagamento de todos os encargos sociais estabelecidos na lei a todo o seu pessoal.

b) O Adjudicatário obriga-se a efetuar apólices de seguro que cobrirão acidentes de trabalho e doenças profissionais, bem como a mantê-las válidas até à conclusão do contrato, nos termos da legislação em vigor.

3. O Adjudicatário obriga-se ainda a segurar os meios de transporte que sejam empregues na Aquisição de serviço, bem como todas as pessoas nelas transportadas na qualidade de passageiros, seja quem for, estas últimas, com valor ilimitado de responsabilidade civil.

4. Os encargos referentes aos seguros impostos por este Caderno de Encargos, bem como qualquer dedução efetuada pela Seguradora a título de franquia, em caso de sinistro indemnizável, serão por conta do Adjudicatário.

5. A Águas do Norte, S.A. pode, sempre que entender conveniente, exigir prova documental da celebração dos contratos de seguro referidos na presente cláusula, devendo o Adjudicatário fornecê-la no prazo 5 (cinco) dias.

CAPÍTULO III
PENALIDADES CONTRATUAIS E RESOLUÇÃO

Cláusula 22.ª
Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a Águas do Norte, S.A. pode exigir do adjudicatário o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:

   a) Pelo incumprimento das datas e prazos de execução dos serviços prestados objeto do contrato, 10% do valor do contrato;

   b) Pelo incumprimento da obrigação de garantia técnica, 5% do valor do contrato;

2. Em caso de resolução do contrato por incumprimento do adjudicatário, a Águas do Norte, S.A. pode exigir-lhe uma pena pecuniária 20% do valor global do contrato.

3. Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo adjudicatário ao abrigo da alínea a) do n.º 1, relativamente aos bens objeto do contrato cujo atraso na entrega tenha determinado a respetiva resolução.

4. Na determinação da gravidade do incumprimento, a Águas do Norte, S.A. tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do adjudicatário e as consequências do incumprimento.

5. A Águas do Norte, S.A. 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 Águas do Norte, S.A. exija uma indemnização pelo dano excedente.

Cláusula 23.ª
Força maior

1. Não podem ser impostas penalidades ao adjudicatário, 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 adjudicatário, na parte em que intervenham;

   b) Greves ou conflitos laborais limitados às sociedades do adjudicatário ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;

   c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo adjudicatário de deveres ou ónus que sobre ele recaiam;

   d) Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;

   e) Incêndios ou inundações com origem nas instalações do adjudicatário 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 adjudicatário não devidas a sabotagem;

g) Eventos que estejam ou devam estar cobertos por seguros;

4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.

5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 24.ª
Resolução por parte da AdNorte

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, a Águas do Norte, S.A. pode resolver o contrato, a título sancionatório, no caso de o adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente nos seguintes casos:
    a) Incumprimento, cumprimento deficiente ou mora no cumprimento de alguma das obrigações compreendidas no presente contrato e que coloquem em crise o normal e adequado funcionamento da instalação;
    b) Declaração do adjudicatário em como não cumprirá alguma obrigação inscrita no presente caderno de encargos e da qual resulte perda do interesse da Águas do Norte, S.A. na prestação contratual.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao adjudicatário e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pela Águas do Norte, S.A..

Cláusula 25.ª
Incumprimento imputável à ÁGUAS DO NORTE, S.A.

Se a Águas do Norte, S.A. praticar ou der causa a facto de onde resulte maior dificuldade na execução do contrato, com agravamento dos encargos respetivos, o adjudicatário tem direito à reposição do equilíbrio financeiro do contrato, nos termos e com os efeitos do disposto nos n.ºs 2 e 3 do artigo 354.º do CCP, que constitui disciplina do presente caderno de encargos.

Cláusula 26.ª

Responsabilidades

O adjudicatário é responsável por todos os danos causados às e nas instalações da Águas do Norte, S.A., a título culposo ou objetivo, que resultem causalmente da sua prestação contratual, ficando constituído na obrigação de indemnizar, aplicando-se o disposto na alínea b), do n.º 1, do artigo 296.º do Código dos Contratos Públicos.

CAPÍTULO IV
RESOLUÇÃO DE LITÍGIOS

Cláusula 27.ª

Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal de Mirandela com expressa renúncia a qualquer outro.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Cláusula 28.ª

Regulamentos dos fornecedores

O Regulamento dos Fornecedores da Águas do Norte, S.A. disponível no site da Águas do Norte, S.A. http://www.adnorte.pt/index.php?id=109 deverá ser integralmente cumprido. Neste Regulamento consta a documentação que deverá ser apresentada, antes de início dos trabalhos e na sua execução.

Cláusula 29.ª

Subcontratação e cessão da posição contratual

1. A Águas do Norte, S.A. pode, a todo o tempo, e mediante mera notificação escrita ao adjudicatário, ceder a sua posição contratual.
2. A cessão e a subcontratação pelo adjudicatário carece de autorização prévia e escrita da Águas do Norte, S.A., sendo admitida nos termos dos artigos do Capítulo VI do CCP.
3. Verificando-se o incumprimento, pelo adjudicatário das suas obrigações assumidas com a celebração do contrato, que preencham os requisitos da resolução do contrato, a Águas

do Norte, S.A. pode, em alternativa à resolução do contrato, ordenar a cedência da posição contratual do adjudicatário ao(s) concorrente(s) do procedimento pré-contratual que precedeu a celebração do contrato em execução, pela ordem sequencial daquele procedimento.

4. Para o efeito previsto na parte final do número anterior, a Águas do Norte, S.A. interpela, gradual e sequencialmente, os concorrentes que participaram no procedimento pré-contratual original, de acordo com a respetiva classificação final, a fim de concluir um novo contrato para a adjudicação da conclusão dos serviços.
5. A execução do contrato ocorre nas mesmas condições já propostas pelo cedente no procedimento pré-contratual original.
6. A cessão da posição contratual opera por mero efeito de ato da Águas do Norte, S.A., sendo eficaz a partir da data por este indicada.
7. Os direitos e obrigações da Águas do Norte, S.A., desde que constituídos em data anterior à da notificação do ato referido no n.º anterior, transmitem-se automaticamente para o cessionário na data de produção de efeitos daquele ato, sem que este a tal se possa opor.
8. As obrigações assumidas pelo cocontratante depois da notificação referida no n.º 6 desta cláusula apenas vinculam a entidade cessionária quando este assim o declare, após a cessão.
9. A caução e as garantias prestadas pelo cedente são objeto de redução na proporção do valor das prestações efetivamente executadas e são liberadas 6 (seis) meses após a data da cessão, ou, no caso de existirem obrigações de garantia, após o final dos respetivos prazos, mediante comunicação dirigida pela Águas do Norte, S.A. aos respetivos depositários ou emitentes.
10. A posição contratual do cedente nos subcontratos por si celebrados transmite-se automaticamente para a entidade cessionária, salvo em caso de recusa por parte desta.

Cláusula 30.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 Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.

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

Cláusula 31.ª

Contagem dos prazos

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

Cláusula 32.ª

Legislação aplicável

O contrato é regulado pela legislação portuguesa.

ANEXO I

AQUISIÇÃO DE SERVIÇOS DE CIBERSEGURANÇA E DE CONFORMIDADE COM A NORMA ISO/IEC27001

1. ENQUADRAMENTO

A Águas do Norte, S.A. é a entidade gestora responsável pelo sistema multimunicipal de abastecimento de água e de saneamento do Norte de Portugal, integrando vários municípios e uma população abrangida de 3,7 (três vírgula sete) milhões de habitantes. No âmbito da sua concessão tem de garantir uma gestão e guarda adequada da informação. Nesse sentido, considerou como estratégico para o seu modelo de negócio, assegurar que a sua estrutura TI e as suas relações com os clientes estejam cobertas por um nível de maturidade máximo em matéria de Segurança da Informação, no respeito pelas diversas normas legais em vigor, incluindo a relativas à da Privacidade e Proteção de Dados.

2. OBJETIVO

Apoiar a implementação de um Centro de Operações de Segurança para acelerar a capacidade de resposta a incidentes e ameaças de cibersegurança. Garantir a atuação do Centro de Operações de Segurança que se baseie na prevenção e na capacidade de detetar riscos e ameaças, assim como reduzir a duração e o impacto de incidentes de segurança que explorem, neguem, degradem ou indisponibilizem os sistemas necessários às operações normais dos negócios.

Prestação de serviços de *Security Officer*, baseada nas melhores práticas do mercado, orientada pela norma ISO/IEC27001, que rege os padrões internacionais da segurança de informação, bem como pelas normativas europeias em sede de Privacidade e Proteção de Dados Pessoais (RGPD).

Os objetivos definidos pretendem garantir a execução de serviços de auditoria e consultoria na área de cibersegurança, de *compliance* (incluindo a preparação da Águas do Norte, S.A. para a certificação ISO/IEC27001, nas componentes que lhe sejam aplicáveis).

A descrição de serviços a apresentar, de auditoria e consultoria de segurança, devem incidir sobre os processos de avaliação, implementação, manutenção, evolução e gestão da plataforma tecnológica/aplicacional da arquitetura desenvolvida pela Águas do Norte, S.A., análise processual de preparação para a certificação ISO/IEC27001 (*compliance*) e serviços, com base em normativos de referência tais como ISO/IEC27001, ISO/IEC27002,

ISO/IEC29100, ISO/IEC20000, ISO/IEC22301, *Open Web Application Security Project*, e por fim, a normativa de privacidade e proteção de dados (RGDP).

3. ÂMBITO

A ampla atividade da Águas do Norte, S.A. obriga a uma evolução e acompanhamento constante de forma a poder responder às necessidades da sua estrutura orgânica com uma maior qualidade de serviço prestado.

O posicionamento da Águas do Norte, S.A. exige uma plataforma tecnológica que garanta a sustentabilidade e disponibilidade dos seus serviços corporativos, tornando-se um requisito de importância vital assegurar a confidencialidade, a integridade e a disponibilidade da informação.

Tendo em consideração as expectativas e exigências da Águas do Norte, S.A., nomeadamente na implementação de um modelo de *Security Officer*, os serviços deverão endereçar as áreas a seguir elencadas.

3.1. Centro de Operações de Segurança

A AdNorte pretende implementar um Centro de Operações de Segurança para acelerar a capacidade de resposta a incidentes e ameaças de cibersegurança.

A atuação do Centro de Operações de Segurança deve basear-se na prevenção e na capacidade de detetar riscos e ameaças, assim como reduzir a duração e o impacto de incidentes de segurança que explorem, neguem, degradem ou indisponibilizem os sistemas necessários às operações normais dos negócios.

A implementação deste projeto pressupõe a adoção de uma solução de gestão de eventos enquanto componente tecnológica chave que permite não só recolher, classificar e avaliar eventos das fontes de dados existentes na rede, mas também executar mecanismos de correlação e priorização de informação relevante.

O Centro de Operações de Segurança deve disponibilizar os meios necessários à correta e eficaz operacionalização dos requisitos decorrentes da Diretiva NIS (network and information security), primeira legislação a nível da União Europeia sobre cibersegurança, que estabelece um conjunto de medidas para prevenir incidentes de cibersegurança na Europa.

O Centro de Operações de Segurança terá as seguintes atividades:

a) Análise da infraestrutura de TI e avaliação de riscos
   - Identificar e avaliar riscos da arquitetura de rede, protocolos de rede e aplicativos em uso;
   - Identificar e avaliar riscos dos sistemas de segurança em uso;
   - Identificar processos de negócios;
   - Definir do Plano de Gestão de Riscos;

b) Definição da arquitetura do Security Operations Center
   - Projeto geral do SOC;
   - Projeto de arquitetura de rede e segurança;
   - Design de informações de segurança e gerenciamento de eventos;
   - Design da plataforma de inteligência artificial cibernética (processos e ações);

c) Implementação e teste do Security Operations Center:
   - Implementação do SOC;
   - Implementação de alterações na arquitetura de rede e segurança;
   - Implementação de informações de segurança e gestão de eventos;
   - Implementação de informações de segurança e gerenciamento de eventos;
   - Design da plataforma de inteligência artificial cibernética - Processos de inteligência de ameaças;
   - Design da plataforma de inteligência artificial cibernética - ações de inteligência de ameaças
   - Teste de resposta de segurança e resiliência.

d) Exercícios do Centro de Operações Internas de Treinamento e Segurança:
   - Treino das equipas de segurança internas;
   - Treino em segurança cibernética e conscientização do utilizador final para utilizadores internos;
   - Exercício de ataque

3.2. AUDIT, CYBERSECURITY & COMPLIANCE ISO/IEC27001

Auditoria de Segurança de Informação – Trata-se de um processo formal de auditoria, que deverá ser realizado de forma abrangente a todos os sistemas/tecnologias de informação em vigor na Águas do Norte, S.A., reproduzindo o nível de segurança (técnica, lógica, funcional e processual baseado no *compliance* ISO/IEC27001) e respetiva análise de

risco em vigor (à data) tendo em consideração a vertente técnica (ex.: análise de vulnerabilidades/ameaças, auditoria de segurança via intrusão externa, etc.). Esta rubrica deverá contemplar três processos em simultâneo:

a) Auditoria de Segurança Externa (identificação & intrusão) - processo de auditoria direcionado aos ativos públicos em vigor na Águas do Norte, S.A. que deverá ser realizado em modelo de "black- box";

b) Auditoria de Segurança Interna - processo realizado à área interna onde deverá ser identificado e correlacionado todos os ativos da Águas do Norte, S.A. e qual o seu nível de maturidade/segurança;

c) Auditoria de *Compliance* ISO/IEC27001 - processo de avaliação de *compliance* num formato transversal sobre todas as áreas corporativas e de negócio da Águas do Norte, S.A. validando os controlos documentais/processuais da norma ISO/IEC27001 em vigor.

Consultoria de Segurança de Informação – processo de consultoria direcionado para o apoio na implementação das recomendações e acompanhamento que a Águas do Norte, S.A. possa necessitar na vertente TI/SI e um plano de evolução para o futuro face às expectativas e exigências da Águas do Norte, S.A..

No *compliance* ISO/IEC27001 pretende-se estabelecer um plano de preparação e conceção de um sistema de gestão de segurança de informação da Águas do Norte, S.A. e apoiar na formação mínima e adequada dos recursos humanos necessários para este efeito.

O processo de consultoria deverá incluir as recomendações e as implementações necessárias para formalização e obtenção da certificação ISO/IEC27001.

4. OBJETIVOS

4.1. CIBERSEGURANÇA

4.1.1. Implementar um Centro de Operações de Segurança para acelerar a capacidade de resposta a incidentes e ameaças de cibersegurança.

4.1.2. Desenvolver um modelo de auditoria e consultoria da segurança para identificar o nível de maturidade TI/SI e respetivo estado atual da segurança de informação (lógica e física) da plataforma tecnológica/aplicacional da Águas do Norte, S.A.. Estabelecendo um referencial de segurança baseado na estratégia de segurança da Águas do Norte, S.A., face ao nível de risco identificado, auxiliando a definição dos próximos passos evolutivos da plataforma TI/SI da Águas

do Norte, S.A., que permita reduzir o risco de segurança e aumentar a credibilidade e estabilidade da sua plataforma TI/SI face à criticidade do seu negócio.

4.1.3. Avaliar o nível de conformidade da plataforma TI/SI, e respetivos resultados obtidos durante o processo, face aos requisitos legais instituídos.

4.1.4. Identificar e detetar possíveis vulnerabilidades existentes, exploráveis a partir da internet ou da rede interna.

4.1.5. Identificar e detetar possíveis ameaças exploráveis a partir da internet ou da rede interna.

4.1.6. Identificar a infraestrutura tecnológica e aplicacional em vigor na Águas do Norte, S.A., estabelecendo o nível de criticidade associado e respetivos requisitos (técnicos, funcionais e de segurança) para monitorização.

4.1.7. Identificar as fontes de informação na vertente de segurança (nomeadamente via estrutura de IDS, *logging* corporativa via Microsoft Active Directory, *logging* via firewall de perímetro).

4.1.8. Planear a evolução do nível de segurança através da definição de projetos a implementar e a respetiva relação de priorização *versus* criticidade.

4.1.9. Determinar limites de investimento de cada projeto, de modo a não comprometer a relação custo/benefício prevista, contribuindo para o orçamento do plano financeiro em TI.

4.1.10. Identificar necessidades de investimento em segurança a curto, médio e longo prazo (plano de evolução versus investimento).

4.1.11. Avaliar o nível de conformidade da plataforma TI/SI, e respetivos resultados obtidos durante o processo, face aos requisitos legais instituídos.

4.1.12. Conhecer o nível de credibilidade e conformidade do processo de evolução estabelecido pela camada de gestão.

4.1.13. Conhecer as vulnerabilidades existentes.

4.1.14. Conhecer os mecanismos de defesa e prevenção de possíveis vulnerabilidades.

4.1.15. Conhecer a infraestrutura tecnológica e aplicacional em vigor na Águas do Norte, S.A., estabelecendo o nível de criticidade associado e respetivos requisitos (técnicos, funcionais e de segurança).

4.1.16. Conhecer as fontes de informação na vertente de segurança (nomeadamente via estrutura de IDS, *logging* corporativa via Microsoft Active Directory, *logging* via firewall de perímetro).

4.1.17. Enquadrar do ponto de vista estratégico os projetos de segurança a implementar face às recomendações evidenciadas no decorrer do processo de auditoria.

4.1.18. Compreender quanto e como é necessário investir em segurança e tecnologia de informação.

4.1.19. Conhecer a relação custo/benefício de projetos de segurança ou tecnológicos.

4.1.20. Conhecer nível de credibilidade e conformidade do processo de evolução estabelecido pela camada de gestão.

4.1.21. Avaliar o nível de cumprimento legal da Diretiva (EU) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível de segurança das redes e da informação em toda a União (*Network and Information Security Directive – NIS*), na Águas do Norte, S.A..

4.2. COMPLIANCE

4.2.1. Avaliar o nível de compliance existente na Águas do Norte, S.A., apoiando a criação de um sistema de gestão de segurança de informação. Esse sistema deverá basear-se na ISO/IEC27001 (e noutras normas relevantes), podendo ou não conduzir à obtenção formal da respetiva certificação.

4.2.2. Apoiar a Águas do Norte, S.A. no desenvolvimento de políticas e normas corporativas de segurança da informação, que abranjam todos os recursos da plataforma tecnológica organizacional. As informações restritas e de interesse exclusivo da Águas do Norte, S.A., que deverão ser tratadas internamente com sigilo absoluto, onde devem receber total proteção.

4.2.3. Avaliar o nível de maturidade TI/SI e de segurança dos sistemas de informação da Águas do Norte, S.A., no que respeita à estrutura de suporte ao negócio, abrangendo as 14 (catorze) áreas da norma ISO/IEC27001:2013.

4.2.4. Identificar as necessidades das áreas de aplicabilidade de políticas e procedimentos, para garantir a conformidade dos processos.

4.2.5. Avaliar e acompanhar o estado do sistema de gestão de segurança de informação através de auditorias internas.

4.2.6. Conhecer o nível de segurança praticado na Águas do Norte, S.A. face à norma internacional.

4.2.7. Proceder à avaliação quantitativa da segurança nas 14 (catorze) áreas identificadas na norma ISO/IEC27001:2013.

4.2.8. Implementar um sistema de gestão de segurança da informação.

4.2.9. Implementar as políticas, procedimentos e normas de segurança da informação, baseado em normativos.

4.2.10. Garantir o funcionamento do sistema de segurança e aplicabilidade de controlos, através de auditorias internas.

5. CYBERSECURITY & COMPLIANCE

5.1. AUDITORIA DE SEGURANÇA DE INFORMAÇÃO FORMAL

5.1.1. A segurança dos sistemas de informação, mais do que um simples produto ou tecnologia que se pode adquirir, aplicar e esquecer, deverá ser encarada como um processo em permanente evolução que requer uma enorme capacidade para provocar e gerir mudanças, tanto nos hábitos e comportamentos como nas infraestruturas organizativas e tecnológicas.

5.1.2. No quadro da presente Caderno de Encargos propõe-se um plano macro, mas com ações muito concretas, que permitam identificar e resolver os problemas existentes, à luz de um critério de gestão de risco compatível com o negócio e a imagem da Águas do Norte, S.A., em linha com o objetivo fundamental de reforçar a sua posição competitiva e preservar os níveis de confiança dos clientes e da comunidade organizacional em geral, incluindo os colaboradores.

5.1.3. Através da execução dos serviços de segurança da informação, deverão ser estabelecidos controlos bem definidos, identificando as principais vulnerabilidades que afetam a plataforma tecnológica de suporte ao negócio da Águas do Norte, S.A., fornecendo uma base sólida para a implementação de princípios que garantam a segurança da informação.

5.1.4. Nesse sentido, e como exemplo, deverão ser realizadas as seguintes ações:

a) Análise da segurança perimétrica (do exterior) baseado em sessões de *pen-testing*;

b) Deteção de vulnerabilidades nas várias plataformas tecnológicas e aplicacionais em vigor, nomeadamente rede de comunicações, equipamentos ativos, sistemas operativos e plataformas aplicacionais;

c) Auditoria de segurança aplicacional;

d) Avaliação do nível de conformidade legal e segurança de informação baseado nas *best-practices* internacionais;

e) Avaliação e diagnóstico do nível de *compliance*, baseado na norma ISO/IEC27001;

f) Avaliação do estado atual da Águas do Norte, S.A. face ao novo regulamento europeu sobre proteção de dados pessoais;

g) Consultoria de segurança da informação.

5.1.5. O processo deve assentar nas melhores práticas e experiência obtidas nos vários processos de auditoria e consultoria realizados nos últimos anos, e visa identificar lacunas de segurança na plataforma tecnológica e aplicacional em funcionamento na Águas do Norte, S.A..

5.2. ANÁLISE DE RISCO

5.2.1. Uma análise de risco é um processo que visa definir em que medida um determinado contexto (que incluí ameaças, vulnerabilidades e o valor a proteger) é ou não aceitável para uma Águas do Norte, S.A..

5.2.2. Na análise de risco que será proposta deverá procurar-se identificar, qualificar e quantificar esses mesmos riscos associados, face aos critérios de aceitação, e aos objetivos considerados como relevantes para a Águas do Norte, S.A.. Os resultados obtidos deverão ser considerados como referência para se identificar os controlos de segurança apropriados a implementar, de forma a mitigar rapidamente os riscos da segurança de informação verificados.

5.2.3. Os processos de análise de risco e respetiva implementação de controlos de segurança deverão ser efetuados de forma periódica, abrangendo ora diversos sectores da Águas do Norte, S.A., ora sistemas de informação específicos.

5.2.4. A análise de risco deve ainda estimar de uma forma sistemática a dimensão e impacto de riscos inerentes à segurança da informação na Águas do Norte, S.A., assim como o processo de comparação entre os riscos estimados face ao critério de determinação do impacto dos mesmos na Águas do Norte, S.A..

5.2.5. A avaliação dos riscos identificados no campo da segurança da informação deverá ter um alcance claramente definido com o objetivo de ser eficaz. Se apropriado, deverá conter a avaliação dos riscos de outras áreas da Águas do Norte, S.A..

5.2.6. Os requisitos de segurança devem ser identificados através de uma avaliação sistemática dos respetivos riscos de segurança.

5.2.7. Os investimentos com a implementação dos controles de segurança deverão ser analisados à luz de critérios de Custo *versus* Benefício, tomando em linha de conta os danos potenciais para o negócio da Águas do Norte, S.A.que poderão resultar de falhas na segurança

5.2.8. A Análise de Risco visa identificar, qualificar e quantificar riscos. Os resultados obtidos versão ser confrontados com critérios de aceitação de risco, e os objetivos relevantes para a Águas do Norte, S.A.. Desta confrontação entre resultados obtidos e critérios de aceitação devem ser extraídas as *guidelines* que permitem definir a forma adequada de gerir os riscos de segurança de informação, e a correta implementação de controlos de proteção.

5.2.9. Uma Análise de Risco corretamente realizada deverá fornecer informações aptas a garantir a Confidencialidade, Disponibilidade e Integridade da Informação, que enquadrarão a Águas do Norte, S.A. numa das situações abaixo.

5.2.10. Uma Análise de Risco deve abranger as seguintes variáveis de processo:

a) Processos de Negócio - Identificação, junto da administração e colaboradores, dos processos de negócio existentes na Águas do Norte, S.A.;

b) Recursos - Identificação dos recursos que serão considerados na análise de risco: pessoas, infraestrutura, aplicações, tecnologia e informação;

c) Vulnerabilidades - Identificação das vulnerabilidades existentes nos recursos que possam causar a indisponibilidade dos serviços ou ser utilizadas para furto de informações;

d) Ameaças - Identificação dos agentes que possam ser considerados ameaça;

e) Impacto - Identificação do impacto que vulnerabilidades e ameaças possam causar à Águas do Norte, S.A. (furto de informação; paralisação de serviços; perdas financeiras, entre outros).

5.3. ÁREAS ABRANGIDAS PELO PROCESSO DE AUDITORIA/CONSULTORIA

5.3.1. A segurança dos sistemas de informação, mais do que um simples produto ou tecnologia que se pode adquirir, aplicar e esquecer, deverá ser encarada de forma integrada com o negócio da empresa, tanto nos hábitos e comportamentos como nas infraestruturas organizativas e tecnológicas.

5.3.2. Através da execução da auditoria de segurança da informação, deverão ser estabelecidos controlos bem definidos, identificando as principais vulnerabilidades que afetam a plataforma tecnológica de suporte ao negócio da Águas do Norte, S.A., fornecendo uma base sólida para a implementação de princípios que garantam a segurança da informação, preparando a Águas do Norte, S.A. para a respetiva certificação na área.

5.3.3. Para o efeito, as áreas abordadas durante a auditoria de segurança, com subáreas específicas, que deverão ser alvo de cuidada atenção, de acordo com o âmbito exposto apresentado, são:

a) Política de Segurança da Informação;

b) ADN da Segurança;

c) Segurança dos Elementos Humanos;

d) Classificação e Controlo dos Recursos de Informação;

e) Controlo de acessos;

f) Criptografia;

g) Segurança Física e Ambiental;

h) Gestão das Operações;

i) Gestão de Comunicações;

j) Manutenção, Desenvolvimento e Aquisição de Sistemas;

k) Relação com Fornecedores;

l) Gestão de Incidentes da Segurança da Informação;

m) Gestão da Continuidade do Negócio;

n) Conformidade;

o) Framework da Privacidade dos Dados.

5.4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5.4.1. Objetivo

Disponibilizar o apoio e a orientação apropriados para a gestão da segurança da informação, de acordo com as exigências e normas em vigor na Águas do Norte, S.A..

5.4.2. Serviço

Análise de procedimentos e políticas de segurança da Informação presentes na Águas do Norte, S.A.:

a) Definição da segurança da informação adequada;

b) Declaração de compromisso da direção;

c) Explanação das políticas de segurança a adotar;

d) Análise crítica e avaliação;

e) Efetividade da política adotada/ a adotar;

f) Análise do custo e impacto associados;

g) Efeitos das mudanças na tecnologia.

5.4.3. Categoria associada à auditoria de segurança

Política de Segurança	Criticidade
Análise de Procedimentos e Políticas de Segurança da Informação presentes na organização	Elevado
Análise Crítica e Avaliação	Elevado

Demonstração de suporte e compromisso da gestão de topo em implementar uma gestão eficaz do risco que paira sobre a informação de negócio. Inclui, entre outras, a abordagem da Águas do Norte, S.A. para as diversas práticas e posturas a tomar por todos os seus recursos humanos.

5.5. ÁGUAS DO NORTE, S.A. DE SEGURANÇA

5.5.1. Objetivo

Gerir a segurança da Informação dentro da Águas do Norte, S.A..

5.5.2. Serviço

Análise da Águas do Norte, S.A. interna:

a) Garantir o compromisso e empenho total da direção nas medidas a tomar para garantir a segurança da informação;

b) Coordenação da segurança da informação;

c) Atribuição de responsabilidades em segurança da informação;

d) Processo de autorização para as instalações de processamento da informação;

e) Acordos de confidencialidade;

f) Consultoria especializada em segurança da informação;

g) Cooperação entre Organizações;

h) Análise crítica Independente de segurança da informação.

Identificação dos riscos no acesso de prestadores de serviços:

a) Identificação dos riscos no acesso de prestadores de serviços;

b) Requisitos de segurança nas transações com Clientes;

c) Requisitos de segurança nas transações com parceiros.

5.5.3. Categoria associada à auditoria de segurança

Águas do Norte, S.A. de Segurança	Criticidade
Análise da Águas do Norte, S.A. Interna	Elevado
Identificação dos riscos no acesso de prestadores de serviços	Crítico

Existência de um fórum ou comité de Segurança da Informação com a participação da gestão de topo, especialistas de segurança e responsáveis pelas diversas áreas de atuação da Águas do Norte, S.A. para debater e planear proactivamente ações a empreender, traçar as políticas de segurança a aplicar em toda a Águas do Norte, S.A., definir as responsabilidades de segurança dos diversos elementos humanos, e definir as condições de segurança da informação a incluir em contratos com terceiros.

5.6. SEGURANÇA DOS ELEMENTOS HUMANOS

5.6.1. Objetivo

Reduzir o risco de erro humano, roubo, fraude ou uso indevido das instalações.

5.6.2. Serviço

Análise da política de recrutamento:

a) Atribuição de cargos e responsabilidades;

b) Acordos de confidencialidade;

c) Termos e condições de trabalho.

Análise do plano de formação:

a) Consciencialização e formação em segurança da informação.

Análise de incidentes e falhas de segurança:

a) Notificação de incidentes e falhas de segurança;

b) Identificação de falhas de sistemas.

Análise de utilização inadequada da informação da Águas do Norte, S.A., por parte dos colaboradores:

a) Existência de processos disciplinares.

5.6.3. Categoria associada à auditoria de segurança

Segurança nos Elementos Humanos	Criticidade
Análise da política de recrutamento	Crítico
Análise do plano de formação	Elevado
Análise de incidentes e falhas de segurança	Elevado
Análise de utilização inadequada da informação da Águas do Norte, S.A., por parte dos colaboradores	Crítico

Desenvolvimento de ações de formação e sensibilização para a problemática da insegurança da informação, a abranger para todos os recursos humanos da Águas do Norte, S.A.. Atribuição de responsabilidades e papéis a desempenhar por cada um dos elementos humanos, face a uma situação de quebra de segurança ou catástrofe.

5.7. CLASSIFICAÇÃO E CONTROLO DOS RECURSOS DE INFORMAÇÃO

5.7.1. Objetivo

Manter a proteção adequada dos ativos da Águas do Norte, S.A..

5.7.2. Serviço realizado

Análise dos recursos de informação:

a) Inventariado dos recursos de informação;

b) Propriedade dos recursos de informação;

c) Utilização correta dos recursos de informação.

Análise da classificação da Informação:

a) Recomendações para a classificação;

b) Classificação e tratamento da informação.

5.7.3. Categoria associada à auditoria de segurança

Classificação e Controlo dos Recursos de Informação	Criticidade
Análise dos recursos de informação	Elevado
Análise da classificação da Informação	Crítico

Existência de um sistema de gestão de inventário de recursos críticos e não críticos da Águas do Norte, S.A., identificação de responsáveis pelo assegurar de uma proteção efetiva ao longo do tempo de vida do recurso, entre outras matérias.

5.8. CONTROLO DE ACESSOS

5.8.1. Objetivo

Controlar o acesso à informação

5.8.2. Serviços

Análise dos sem monitorização.

Análise do acesso à plataforma aplicacional:

a) Restrições de acesso à informação;

b) Isolamento de sistemas críticos.

Análise dos requisitos do negócio para controlo de acessos:

a) Política de controlo de acessos.

5.8.3. Categoria associada à auditoria de segurança

Controlo de Acessos	Criticidade
Análise dos requisitos do negócio para controlo de acessos	Elevado
Análise de segurança nos acessos dos utilizadores	Crítico
Análise das responsabilidades dos utilizadores	Crítico
Análise do acesso à plataforma aplicacional	Crítico
Análise dos acessos aos recursos de rede	Crítico
Análise do acesso e autenticação aos sistemas	Elevado
Monitorização do uso e acesso aos sistemas	Elevado
Análise de comunicações móveis	Crítico

5.8.4. Serviço realizado

Análise dos requisitos do negócio para controlo de acessos:

a) Política de controlo de acessos.

Análise dos acessos aos recursos de rede:

a) Política de utilização de recursos de rede.

Autenticação para ligações externas:

a) Proteção de portas de diagnóstico e configuração remotas;

b) Segregação de redes;

c) Controlo de ligações de rede;

d) Segurança dos serviços de rede.

Análise do Acesso e Autenticação aos sistemas:

a) Procedimentos de autenticação segura;

b) Identificação e autenticação do utilizador;

c) Sistema de gestão de *passwords*;

d) Uso restrito de utilitários do sistema;

e) *Session* time-out;

f) Limitação do período de acesso aos sistemas.

5.8.5. Categoria associada à auditoria de segurança

Controlo de Acessos	Criticidade
Análise dos requisitos do negócio para controlo de acessos	Elevado
Análise de segurança nos acessos dos utilizadores	Crítico
Análise das responsabilidades dos utilizadores	Crítico
Análise do acesso à plataforma aplicacional	Crítico
Análise dos acessos aos recursos de rede	Crítico
Análise do acesso e autenticação aos sistemas	Elevado

5.8.6. Serviço realizado

Monitorização do uso e Acesso aos sistemas:

a) Registo de eventos (*logs* do sistema);

b) Monitorização do uso do sistema;

c) Sincronização dos relógios.

Análise de Comunicações Móveis:

a) Trabalho remoto;

b) Acessos remotos.

5.8.7. Categoria associada à auditoria de segurança

Controlo de Acessos	Criticidade
Monitorização do uso e acesso aos sistemas	Elevado
Análise de comunicações móveis	Crítico

Definição de controlos que permitam assegurar que determinada informação, é acessível apenas por aqueles que possuem as devidas credenciais.

5.9. SEGURANÇA FÍSICA E AMBIENTAL

5.9.1. Objetivo

Prevenir acessos não autorizados, prejuízos e interposição à informação e instalações físicas da Águas do Norte, S.A..

5.9.2. Serviço realizado

Análise de segurança de áreas:

a) Perímetro de segurança física;

b) Controlos de entrada física;

c) Condições de segurança das instalações;

d) Isolamento de áreas críticas.

Análise de segurança dos equipamentos:

a) Instalação e proteção de equipamentos;

b) Condições de fornecimento de energia;

c) Verificação de condições de segurança da cablagem estruturada de comunicações;

d) Manutenção de equipamentos;

e) Reutilização e alienação de equipamentos.

5.9.3. Categoria associada à auditoria de segurança

Segurança Física e Ambiental	Criticidade
Análise de segurança de áreas	Elevado
Análise de segurança dos equipamentos	Crítico

Definição concreta e concisa do modelo de segurança física e ambiental a implementar para controlo e segurança de locais e pessoas, com base em requisitos identificados.

5.10. GESTÃO DAS OPERAÇÕES E COMUNICAÇÕES

5.10.1. Objetivo

Garantir o funcionamento seguro e correto dos recursos de processamento da informação.

5.10.2. Serviço

Análise de procedimentos e responsabilidades operacionais:

a) Documentação de procedimentos de operação;

b) Controlo de mudanças operacionais;

c) Procedimento para a gestão de incidentes;

d) Segregação de funções;

e) Separação dos ambientes de desenvolvimento e de produção;

f) Gestão de recursos externos.

Análise do planeamento e aprovação de sistemas:

a) Planeamento de capacidade;

b) Aceitação de sistemas.

Análise da proteção existente contra *software* malicioso:

a) Controlos contra *software* malicioso.

5.10.3. Categoria associada à auditoria de segurança

Gestão das Operações e Comunicações	Criticidade
Análise de procedimentos e responsabilidades operacionais	Elevado
Análise do planeamento e aprovação de sistemas	Crítico
Análise da proteção existente contra *software* malicioso	Crítico
Análise de políticas de *Backup* & *Restore*	Crítico
Análise da segurança de rede	Crítico
Segurança e Manutenção dos medias de *Backup*	Elevado
Análise de permutas de informação	Crítico

5.10.4. Serviço realizado

Análise da segurança de Rede:

a) Controlos de rede;

b) Segurança de serviços de rede.

Análise de políticas de *Backup* & *Restore*:

a) Cópias de segurança;

b) Registo de operações (*Backup* & *Restore*);

c) Registo de falhas.

Segurança e Manutenção dos medias de *Backup*:

a) Gestão dos *medias*;

b) Exclusão de *medias*;

c) Procedimento de gestão da informação guardada;

d) Segurança da documentação dos sistemas.

Análise de permutas de Informação:

a) Políticas e procedimentos para a permuta de informação;

b) Segurança de *medias* em circulação;

c) Segurança de comércio eletrónico;

d) Segurança de correio eletrónico;

e) Segurança de sistemas de informação.

5.10.5. Categoria associada à auditoria de segurança

Gestão das Operações e Comunicações	Criticidade
Análise de procedimentos e responsabilidades operacionais	Elevado
Análise do planeamento e aprovação de sistemas	Crítico
Análise da proteção existente contra *software* malicioso	Crítico
Análise de políticas de *Backup & Restore*	Crítico
Análise da segurança de rede	Crítico
Segurança e Manutenção dos medias de *Backup*	Elevado
Análise de permutas de informação	Crítico

Planeamento do desenvolvimento de uma postura comunicativa eficaz que otimize a gestão das operações de sistemas e redes de comunicações. Definição de procedimentos de operação e de segurança dos equipamentos, gestão de alterações, segregação de ambientes de desenvolvimento e produção, planeamento e gestão de capacidades, cópias de segurança, entre outros.

5.11. MANUTENÇÃO, DESENVOLVIMENTO E AQUISIÇÃO DE SISTEMAS

5.11.1. Objetivo

Garantir que a segurança é parte integrante dos sistemas de informação.

5.11.2. Serviço realizado

Análise dos requisitos de segurança de sistemas:

a) Análise e especificação dos requisitos de segurança.

Análise de segurança nos sistemas aplicacionais:

a) Validação de dados (entrada e saída);

b) Controlo de processamento interno.

Controlo criptográfico:

a) Política para o uso de controlos de criptografia;

b) Criptografia, assinatura digital e gestão de chaves.

Análise da segurança de ficheiros de sistema:

a) Controlo de software em produção;

b) Proteção de dados de teste do sistema.

Análise da segurança dos processos de desenvolvimento e suporte:

a) Procedimentos de controlo de alterações;

b) Análise crítica das alterações do sistema em produção;

c) Fuga de informação.

5.11.3. Categoria associada à auditoria de segurança

Manutenção, Desenvolvimento e Aquisição de Sistemas	Criticidade
Análise dos requisitos de segurança de sistemas	Elevado
Análise de segurança nos sistemas aplicacionais	Crítico
Controlo criptográfico	Crítico
Análise da segurança de ficheiros de sistema	Crítico
Análise da segurança dos processos de desenvolvimento e suporte	Elevado

Assegurar que projetos de tecnologias de informação e atividades de suporte são desde início conduzidos tendo em conta a segurança da informação e respeitando as políticas em vigor na Águas do Norte, S.A..

5.12.GESTÃO DE INCIDENTES DA SEGURANÇA DA INFORMAÇÃO

5.12.1. Objetivo

Assegurar que os registos de eventos de segurança (*logs*) e lacunas associadas com os sistemas de informação são reportados de forma a serem devidamente corrigidas.

5.12.2. Serviço realizado

Análise dos Incidentes de Segurança e lacunas associadas com os Sistemas de Informação:

a) Registo de incidentes de segurança;

b) Registo de lacunas de segurança.

Análise da Gestão de Incidentes de Segurança e respetivas correções:

a) Procedimentos e competências;

b) Aprendizagem da informação dos incidentes de segurança;

c) Recolha de evidências.

5.12.3. Categoria associada à auditoria de segurança

Segurança na Gestão de Incidentes da Segurança da Informação	Criticidade
Análise dos incidentes de segurança e lacunas associadas com os sistemas de informação	Elevado
Análise da gestão de incidentes de segurança e respetivas correções	Elevado

Assegurar que procedimentos de escalonamento e *reporting* de incidentes são devidamente implementados na Águas do Norte, S.A.. Todos os colaboradores, parceiros de negócio e empresas externas que prestem serviços à Águas do Norte, S.A. devem ter conhecimento dos procedimentos implementados, para que de uma forma rápida e adequada possam reportar às pessoas indicadas diferentes tipos de lacunas e incidentes detetados com potencial impacto na segurança dos recursos da informação

5.13. GESTÃO DA CONTINUIDADE DE NEGÓCIO

5.13.1. Objetivo

Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos.

5.13.2. Serviço realizado

a) Análise dos aspetos da gestão da continuidade do negócio:

b) Processo de gestão da continuidade do negócio;

c) Continuidade do negócio e análise do impacto;

d) Implementação de planos de continuidade;

e) Teste, manutenção e avaliação dos planos de continuidade do negócio.

5.13.3. Categoria associada à auditoria de segurança

Segurança na Gestão da Continuidade do Negócio	Criticidade
Análise dos aspetos da gestão da continuidade do negócio	Elevado

Desenvolvimento de processos que permitam a gestão continuada e melhoria contínua de planos de contingência que protejam os processos críticos de negócio dos riscos existentes.

5.14.CONFORMIDADE

5.14.1. Objetivo

Evitar a violação de lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.

5.14.2. Serviço realizado

Análise da Conformidade com requisitos Legais:

a) Identificação da legislação vigente;

b) Direitos de propriedade e de autor;

c) Salvaguarda de registos organizacionais;

d) Proteção de dados e privacidade da informação pessoal;

e) Prevenção contra uso indevido de recursos corporativos;

f) Regulamentação de controlos de criptografia;

g) Registo de evidências.

Análise crítica da política de Segurança e da Conformidade técnica:

a) Conformidade com a política de segurança;

b) Verificação da conformidade técnica.

Análise e considerações quanto à Auditoria de sistemas:

a) Controlos de auditoria de sistemas;

b) Proteção de ferramentas de auditoria de sistemas.

5.14.3. Categoria associada à auditoria de segurança

Controlo da Conformidade	Criticidade
Análise da conformidade com requisitos legais	Elevado
Análise crítica da política de segurança e da conformidade técnica	Crítico
Análise e considerações quanto à auditoria de sistemas	Elevado

Capacidade de demonstração de compromisso a todos os elementos humanos da Águas do Norte, S.A., Clientes, fornecedores, e autoridades externas, relativamente ao cumprimento de normativos legais e outras normas, internas ou externas, relacionadas com a informação.

5.15.AUDITORIA DE SEGURANÇA DE INFORMAÇÃO FORMAL

5.15.1. Uma melhoria do nível de segurança de informação da Águas do Norte, S.A. terá de ser garantida através de um processo de reestruturação organizacional (pessoas, processos e tecnologia). Contudo, e de forma a controlar e manter em linha os objetivos estratégicos da camada de gestão em vigor, é fundamental uma componente ativa de controlo sobre a evolução da plataforma TI/SI de suporte ao negócio. Nesse sentido, o Adjudicatário, deverá definir e executar um plano de auditorias formais de segurança de informação com uma periodicidade adequada ao negócio da Águas do Norte, S.A..

5.15.2. Os resultados (qualitativos e quantitativos) face às métricas e controlos definidos previamente servirão de base estrutural para refinar o plano de evolução, e enquadrar a estratégia global da Águas do Norte, S.A. com o seu nível de segurança e exigências do modelo de negócio em vigor. Adicionalmente, o processo de auditoria servirá para passar o conhecimento sobre o nível de segurança da Águas do Norte, S.A. e, respetiva exposição ao risco, para a camada de gestão e estrutura acionista da Águas do Norte, S.A..

5.15.3. Desta forma, será possível garantir um nível de segurança adequado face à criticidade do negócio em causa, e um grau elevado de credibilidade da imagem institucional da Águas do Norte, S.A. no panorama nacional e internacional.

5.15.4. Consultoria de Segurança de Informação

5.15.4.1. Para que o processo de evolução do nível de segurança de informação e maturidade das plataformas tecnológicas e aplicacionais da Águas do Norte, S.A. seja efetivo, é fundamental a participação de uma entidade externa idónea, independente da Águas do Norte, S.A., devidamente especializada em segurança de informação, para execução do processo de auditoria.

5.15.4.2. A entidade auditora terá a responsabilidade de apoiar a camada de gestão e direções associadas na definição e execução da estratégia para os sistemas de informação da

Águas do Norte, S.A., garantindo um acréscimo de conhecimento e *know-how* técnico de acordo com as exigências legais e de segurança. Para tal, deverá acompanhar o processo de implementação das recomendações de segurança, procurando garantir o cumprimento do mesmo.

5.15.4.3. Da mesma forma, e face à necessidade de interligação constante com redes e modelos de negócio paralelos (parceiros, entidades externa e utentes), a entidade auditora deverá, adicionalmente, validar a conformidade das mesmas de acordo com as boas praticas e norma de referência (ISO/IEC27001) salvaguardando sempre os interesses e objetivos da Águas do Norte, S.A. e o alinhamento das decisões com a sua estratégia

5.16.SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

5.16.1. A realidade demonstra que nenhuma Instituição pode assumir que está totalmente protegida das ameaças que colocam em risco a sua informação. O risco que impende sobre a Informação pode no entanto ser gerido e mitigado, através de um sistema de gestão da segurança da informação baseado em referenciais reconhecidos (ISO/IEC27001, ISO/IEC27002), que incorpore a estrutura organizacional, as pessoas que a compõem e os processos que desenvolve.

5.16.2. Um Sistema de Gestão da Segurança da Informação (SGSI) é um sistema de gestão baseado numa aproximação sistemática aos riscos inerentes ao negócio, com o objetivo de estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação. Trata-se de uma abordagem da segurança da informação numa perspetiva organizacional.

5.16.3. O SGSI permite implementar controlos com o objetivo de minimizar os riscos. Através de uma metodologia interativa, os riscos são analisados e mitigados por controlos selecionados de acordo com as melhores práticas da indústria, sendo a eficácia da sua implementação validada através de auditorias regulares numa perspetiva de melhoria contínua.

5.16.4. A norma ISO/IEC27001 e ISO/IEC27002 define a sua abordagem como a aplicação de um sistema de processos dentro de uma Águas do Norte, S.A., juntamente com a identificação e interações entre esses processos e a sua gestão. O SGSI emprega o modelo (PDCA, *Plan-Do-Check-Act*) para estruturar os processos de gestão de segurança de informação, de modo a garantir a melhoria contínua da proteção dos ativos da Águas do Norte, S.A..

5.16.5. Com base no ciclo "*Plan-Do-Check-Act*":

a) *Plan* = onde se definem os requisitos, se avalia os riscos e se decide quais os controlos adequados;

b) *Do* = onde se implementa e opera o SGSI;

c) *Check* = onde se acompanha e analisa o SGSI;

d) *Act* = onde se mantém e melhora continuamente o SGSI.

5.16.6. O SGSI também define alguns documentos específicos que são necessários e devem ser controlados, e garante a gestão dos registos que comprovam a operação do SGSI.

5.16.7. Responsabilidade da Gestão

A gestão deve demonstrar o seu compromisso com o SGSI, principalmente através da atribuição de recursos suficientes para implementar e operar.

5.16.8. Auditorias Internas

A Águas do Norte, S.A. deve realizar auditorias internas periódicas para assegurar que o SGSI incorpora controlos adequados e que operem de forma eficaz.

5.16.9. Análise da Gestão

A gestão deve analisar a pertinência, a adequação e a eficácia do SGSI, pelo menos uma vez por ano, identificando eventuais oportunidades de melhoria e avaliando a necessidade de mudança.

5.16.10. Melhorias

A Instituição deve melhorar continuamente o SGSI, através da avaliação e se necessário fazer mudanças para garantir a sua adequação e eficácia, gerindo-se não-conformidades de modo a evitar possíveis problemas recorrentes.

5.17.FATORES DE SUCESSO PARA A IMPLEMENTAÇÃO

5.17.1. Para o sucesso da implementação de um Sistema de Gestão de Segurança de Informação, é importante alinhar os seguintes vetores:

5.17.2. Comprometimento da Gestão de Topo

A Gestão de Topo da Águas do Norte, S.A. deve estar envolvida no Sistema de Gestão, assegurando, nomeadamente:

a) Representação na Comissão de Segurança;

b) Aprovação dos documentos elaborados no âmbito do SGSI;

c) Apoio na Implementação dos processos e procedimentos de Segurança de Informação, nomeadamente dos investimentos necessários;

d) Revisão periódica do estado do SGSI, no que se refere ao cumprimento de objetivos e mitigação de Não Conformidades.

5.17.3. Comprometimento das Áreas

Todas as áreas envolvidas na definição e implementação dos processos associados ao SGSI devem encontrar-se disponíveis para a sua definição e implementação.

5.17.4. Comprometimento de todos os Colaboradores

Todos os colaboradores devem ser sensibilizados para a importância da informação e sua segurança, bem como para o cumprimento dos procedimentos implementados para a Segurança de Informação.

5.17.5. Definição do responsável pela implementação do SGSI

É necessária a alocação de um Recurso Humano dedicado a tempo inteiro à Implementação do SGSI e posterior monitorização e acompanhamento.

5.18.SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

5.18.1. A informação e os seus processos de apoio, sistemas e redes, são bens essenciais ao negócio de uma Águas do Norte, S.A.. Confidencialidade, Integridade e Disponibilidade da informação, são elementos essenciais para preservar a competitividade, rentabilidade e a respetiva imagem da Águas do Norte, S.A. no mercado.

5.18.2. Tendo em consideração as expectativas da Águas do Norte, S.A., nomeadamente no apoio à conceção e desenvolvimento de práticas de Gestão de Risco e da Segurança da Informação, os serviços deverão endereçar no que se refere à definição do Sistema de Gestão de Segurança da Informação:

a) Realização de uma avaliação (*assessment*) às práticas de (gestão) segurança da informação nas unidades orgânicas e direções de serviço da Águas do Norte, S.A., usando como modelo de referência as normas internacionais ISO/IEC27001 e ISO/IEC27002;

b) Aplicação de questionários de avaliação de comportamentos dos colaboradores da utilização de recursos de informação;

c) Desenvolvimento de políticas, procedimentos para a segurança da informação;

d) Obtenção do envolvimento e do comprometimento do universo dos utilizadores da Águas do Norte, S.A. para os temas da Gestão de Segurança da Informação;

e) Implementação do Sistema de Gestão de Segurança da Informação (SGSI) com base nos requisitos e orientações das normas internacionais ISO/IEC27001 e ISO/IEC27002. Para tal, será necessário estabelecer o modelo de Águas do Norte, S.A. de segurança da informação, bem como definir estrutura de funções, autoridades, responsabilidades e competências de gestão de segurança da informação;

f) Realização de *workshops* de sensibilização à segurança da informação;

g) Realização de auditoria interna para verificar a eficácia da implementação do SGSI.

5.19.REQUISITOS PARA A CERTIFICAÇÃO

Requisitos necessários para obter a certificação de um Sistema de Segurança de Informação:

a) Implementação do SGSI: Definição do âmbito do SGSI, bem como das políticas e procedimentos. Estes devem ser ajustados à realidade da Águas do Norte, S.A. e implementados em conformidade com a norma, bem como com as leis em vigor;

b) Auditoria Interna ao SGSI: Deve existir uma auditoria, no mínimo anual, ao sistema. Esta auditoria é obrigatória no âmbito do processo de certificação e deverá ocorrer antes do mesmo;

c) Auditoria de Certificação: É composta por duas fases, uma processual e outra de verificação e *compliance*.

6. REQUISITOS MININOS DO PERFIL DOS RECURSOS A DISPONIBILIZAR

6.1. PERFIL GESTOR DO PROJETO

a) Curso superior nas áreas de Engenharia Informática, Engenharia Eletrotécnica ou equivalente na área de Sistemas e Tecnologias de Informação;

b) Experiência comprovada (mínima de 5 anos, aceitando-se poder ser em diferentes empresas) em projetos de consultoria, auditoria em segurança informática;

c) Project Management Professional

d) Auditor de segurança credenciado pelo Gabinete Nacional de Segurança;

e) *Lead Auditor* e *Lead Implementar* na norma ISO/IEC27001;

f) Membro da IAPP – *The International Association of Privacy Professionals*.

6.3 PERFIL GESTOR TÉCNICO

6.3.1 Administrador de redes e comunicações

a) Experiência comprovada no mínimo de 7 (sete) anos;

b) Certificação Cisco IP NGN System Engineer Representative;

c) Experiência comprovada na implementação de QoS (Quality of Service) em redes locais (wired e wireless) e redes alargadas;

d) Experiencia comprovada na implementação de protocolos BGP (redes privadas e redes públicas);

e) Experiência comprovada em pelo menos duas implementações de soluções de networking de âmbito Nacional;

f) Experiência comprovada na gestão e configuração em soluções de switching (core e distribuição), Routing e Wireless em cenários empresariais e distribuídos geograficamente.

6.3.3 Administração de plataformas Check Point

a) Licenciatura nas áreas de Engenharia Informática, Engenharia Eletrotécnica ou na Área de Sistemas e Tecnologias de Informação;

a) Experiência profissional mínima de 7 (sete) anos em administração de soluções de segurança;

b) Certificação Check Point Certified Expert (CCSE ou superior) válida comprovada;

6.3.4 Administração de plataformas Barracuda Web Application Firewall

a) Licenciatura nas áreas de Engenharia Informática, Engenharia Eletrotécnica ou na Área de Sistemas e Tecnologias de Informação;

b) Experiência profissional mínima de 7 (sete) anos em administração de soluções de segurança;

c) Certificação comprovada "Barracuda Web Application Firewall Certified Engineer"

6.2. PERFIL – CENTRO DE OPERAÇÕES DE CIBERSEGURANÇA

a) Curso superior nas áreas de Engenharia Informática, Engenharia Eletrotécnica ou equivalente na área de Sistemas e Tecnologias de Informação;

6.3. PERFIL – SERVIÇOS DE CIBERSEGURANÇA

a) Experiência comprovada (mínima de 5 anos, aceitando-se poder ser em diferentes empresas) em projetos de cibersegurança.

6.4. PERFIL – AUDIT, COMPLIANCE, CIBERSEGURANÇA

a) Curso superior nas áreas de Engenharia Informática, Engenharia Eletrotécnica ou equivalente na área de Sistemas e Tecnologias de Informação;

b) Experiência comprovada do técnico (mínima de 6 anos, aceitando-se poder ser em diferentes empresas) em segurança dos sistemas de informação;

c) Responsável por mais de 5 (cinco) projetos de auditoria;

d) Experiência na implementação de processo de segurança física, privacidade de dados, segurança de infraestruturas, cumprimento da norma ISO/IEC270001;

e) *Manager Certificate in IT Service Management* (ITIL);

f) *Lead Auditor* e *Lead Implementar* na norma ISO/IEC27001 (Certificação ISO 27001 Foundation);

g) Experiência e especialização no domínio da gestão e implementação de Sistemas de Informação;

h) *Microsoft Certified Systems Engineer* (MCSE 2003, MCSE Messaging, MCSE Security);

i) Experiência profissional em projetos de elevada complexidade, nomeadamente em plataformas Micorsoft, HP, Cisco e outras;

j) Forte experiência em testes de Intrusão Físico e Lógico;

k) Forte experiencia na implementação de Sistemas de Segurança de Informação (Windows, Unix);

l) *Certified Ethical Hacker* (CEH);

m) *Certified Ethical Instructor* (CEI);

n) (Microsoft Certified Solutions Expert ++

o) Microsoft Certified Solutions Associate ++

p) VMware Certified Professional - Data Center Virtualization 2020 ++

6.5. PERFIL – JURÍDICO-LEGAL

a) Licenciatura em Direito;

b) Certificação de DPO;

c) Experiência em proteção de dados pessoais.

7. FUNÇÕES PRINCIPAIS

7.1. GESTOR DO PROJETO

Terá a responsabilidade de planear e controlar a execução do projeto.

7.2. GESTOR TÉCNICO

Terá a responsabilidade técnica do projeto apoiando sempre que necessário a atividades desenvolvidas no centro de operações.

7.3. CENTRO DE OPERAÇÕES DE CIBERSEGURANÇA

a) Terá a responsabilidade de prestar serviços de deteção e reação a incidentes de segurança.
b) Registar e tratar os incidentes.
c) Corrigir falhas de segurança.
d) Administrar plataformas de segurança Checkpoint, Barracuda (WAF), Kaspersky
e) Monitorizar a rede através de plataformas (PRTG e Cisco)
f) Verificação de vulnerabilidade através de ferramentas (OpenVAS ou equivalente)
g) Elaborar relatórios mensais.

7.4. SERVIÇOS DE CIBERSEGURANÇA

Apoiar quinzenalmente as atividades desenvolvidas pelo centro de operações de cibersegurança

7.5. PERFIL – AUDIT, COMPLIANCE, CIBERSEGURANÇA

Serviços de auditoria, COMPLIANCE, CIBERSEGURANÇA, incluindo a preparação da Águas do Norte, S.A. para a certificação ISO/IEC27001, nas componentes que lhe sejam aplicáveis – Uma visita mensal

8. LOCAIS PARA PRESTAÇÃO DOS SERVIÇOS

	Descrição dos Serviços	Locais
1	Serviços Centro de Operações – Um recurso dedicado, 11 meses por ano em horário útil	Barcelos
2	Serviços de CIBERSEGURANÇA, para apoiar serviços previstos no ponto 1 – Uma visita quinzenal	Vila Real e Barcelos
3	Serviços de AUDIT, COMPLIANCE, CIBERSEGURANÇA, incluindo a preparação da Águas do Norte, S.A. para a certificação ISO/IEC27001, nas componentes que lhe sejam aplicáveis – Uma visita mensal	Vila Real
4	Serviços de Reconhecimento da Infraestrutura AdNorte	Vila Real e Barcelos