



ÁGUAS E RESÍDUOS DA MADEIRA



CONCURSO PÚBLICO
(COM PUBLICIDADE NACIONAL)

N.º 01.0885

**“SERVIÇOS DE CIBESSEGURANÇA SOCAAS (SECURITY
OPERATIONS CENTER AS A SERVICE) - 2º PROCEDIMENTO”**

CADERNO DE ENCARGOS

CADERNO DE ENCARGOS

Capítulo I Disposições gerais

Cláusula 1.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 realização de serviços de Cibersegurança, nomeadamente os referenciados como “**Security Operations Center – SOC**”, em conformidade com o previsto no anexo I - Características do serviço a prestar do presente caderno de encargos e respetivos anexos.

Cláusula 2.ª

Preço Base

O preço base é o preço máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o seu objeto, sendo que no presente procedimento corresponde a **128.000,00 €** (cento e vinte e oito mil euros), valor ao qual acresce o IVA à taxa legal em vigor.

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 suprimimentos dos erros e das omissões do Caderno de Encargos identificados pelos concorrentes, 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.

Cláusula 4.ª

Prazo

O contrato mantém-se em vigor **pelo prazo máximo de 26** (vinte e seis) **meses**, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato, estando dividido pelos seguintes prazos:



ÁGUAS E RESÍDUOS DA MADEIRA



- i) **O prazo de implementação dos serviços será no máximo de 2 (dois) meses, após a celebração do contrato.**
- ii) **Os serviços “Security Operations Center – SOC” decorrem no prazo de 24 (vinte e quatro) meses, a contar do termo da implementação dos serviços, e entrada em serviço.**

Capítulo II

Obrigações contratuais

Secção I

Obrigações do prestador de serviços

Subsecção I

Disposições gerais

Cláusula 5.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 decorrem para o prestador de serviços as seguintes obrigações principais:

- a) Efetuar setup do serviço implementado e uso de todos os componentes necessários para boa prestação do mesmo, conforme especificado no Anexo I do presente caderno de encargos;
- b) Monitorizar os eventos gerados na rede da ARM, S.A. conforme especificados no Anexo I do presente caderno de encargos;
- c) Classificar os eventos recolhidos e assinalar os que podem configurar incidentes de CiberSegurança;
- d) Implementar automatismos para a contenção (SOAR).
- e) Participar e auxiliar as equipas da ARM, S.A. nas fases de erradicação e recuperação de incidentes de CiberSegurança;
- f) Colaborar com a ARM, S.A. na resolução de problemas e vulnerabilidades que afetem a segurança das redes;
- g) Elaborar os relatórios periódicos conforme definido no Anexo I do presente caderno de encargos;
- h) Obrigação de garantia do serviço prestado.

2 — A título acessório, o prestador de serviços fica ainda 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.

Cláusula 6.ª

Forma da prestação do serviço

A prestação dos serviços de consultoria de suporte do software deverá obedecer às características principais descritas nos anexos ao presente Caderno de Encargos.

Cláusula 7.ª

Pessoal

Este serviço deverá ser assegurado por pessoal devidamente qualificado, por forma a permitir a realização de um serviço de elevada qualidade e em conformidade com o Código dos Contratos Públicos e demais legislação aplicável.

Cláusula 8.ª

Receção dos elementos a produzir ao abrigo do contrato

1 — No prazo de 30 dias a contar da entrega dos relatórios periódicos previstos na alínea g) do n.º 1 da cláusula 5.ª, a ARM, S.A. procede à respetiva análise, com vista a verificar se os mesmos foram realizados de acordo com os requisitos definidos no anexo I do presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.

2 — Na análise a que se refere o número anterior, o prestador de serviços deve prestar à ARM, S.A. toda a cooperação e todos os esclarecimentos necessários.

3 — No caso de a análise da ARM, S.A. a que se refere o n.º 1 não comprovar a conformidade dos elementos entregues, ou no caso de existirem discrepâncias em relação aos requisitos técnicos definidos no anexo I ao presente Caderno de Encargos, a ARM, S.A. deve disso informar, por escrito, o prestador de serviços.

4 — No caso previsto no número anterior, o prestador de serviços deve proceder, à sua custa e no prazo razoável que for determinado pela ARM, S.A. às alterações e complementos necessários para garantir o cumprimento das exigências e requisitos técnicos exigidos.

5 — Após a realização das alterações e complementos necessários pelo prestador de serviços, no prazo respetivo, a ARM, S.A. procede a nova análise, nos termos do n.º 1.

6 — Caso a análise da ARM, S.A. a que se refere o n.º 1 comprove a conformidade dos elementos entregues pelo prestador de serviços com as exigências legais, e neles não sejam detetadas quaisquer discrepâncias em relação aos requisitos técnicos definidos no anexo I ao presente Caderno de Encargos, deve ser emitida, no prazo máximo de 5 dias a contar do termo dessa análise, declaração de aceitação pela ARM, S.A..

7 — A emissão da declaração a que se refere o número anterior não implica a aceitação de eventuais discrepâncias com as exigências legais ou com os requisitos técnicos previstos no anexo I ao presente Caderno de Encargos.

Subsecção II

Dever de sigilo

Cláusula 9.ª

Objeto do dever de sigilo

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



ÁGUAS E RESÍDUOS DA MADEIRA



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 prestador de serviços 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 10.ª

Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor até ao termo **do prazo de 3 (três) 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.

Secção II

Obrigações da ARM, S.A.

Cláusula 11.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 ARM, S.A. 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 ARM, S.A, incluindo **as despesas referentes a meios humanos, despesas de transporte, de aluguer de viaturas, de alimentação, de viagens e de estadia, bem como quaisquer encargos decorrentes da atividade exercida durante a prestação de serviços e da utilização de marcas registadas, patentes ou licenças.**

Cláusula 12.ª

Condições de pagamento

1 - A quantia devida pela ARM, S.A., nos termos da cláusula anterior, **deve ser paga no prazo máximo de 30 a 60 dias após a receção pela ARM, S.A. das respetivas faturas**, as quais só podem ser emitidas após o vencimento da obrigação respetiva.

2 - Para efeitos do número anterior, a obrigação considera-se vencida no final de cada mês, mas somente após a implementação e entrada em serviço.

3 — Em caso de discordância por parte da ARM, S.A., quanto à conformidade da fatura emitida, deve esta comunicar ao cocontratante, por escrito, os respetivos fundamentos, ficando o cocontratante obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

4 - O cocontratante não poderá ceder quaisquer direitos ou obrigações emergentes do presente contrato, incluindo a cessão de créditos, sem a prévia autorização escrita, por qualquer meio registado, da ARM; S.A..



ÁGUAS E RESÍDUOS DA MADEIRA



5 - Em caso de violação do disposto no número anterior, incluindo a realização de uma cessão de créditos com a expressa oposição da ARM, S.A., o cocontratante será responsável por todos os custos acrescidos que o cumprimento da obrigação perante o cessionário acarretar para o contraente público.

Capítulo III Penalidades contratuais e Resolução

Cláusula 13.ª

Penalidades contratuais

1 – Pelo incumprimento de obrigações emergentes do contrato, a ARM, S.A. pode exigir do prestador de serviços o pagamento de uma pena pecuniária até 5% do respetivo preço contratual, sem prejuízo do direito de resolução sancionatória do contrato, caso o início da resolução das situações colocadas não seja feita dentro dos prazos fixados na respetiva proposta e/ou essa resolução não seja concluída por forma a que a ARM, S.A. consiga cumprir com os seus prazos legais e contratuais.

2 – Penalidades por incumprimento do estipulado em SLA:

Falha	Penalidade	Nota
Falha em deteção de ciberataque (real ou simulado), por provada insuficiência do Serviço SOC contratado	5% do preço contratual	
Violação da taxa de concretização mínima no tempo de comunicação ao cliente em caso de incidente conforme definido no SLA	$((100\% - \% \text{concretização}) / 100 \times \text{Valor da Mensalidade})$ (ex: uma taxa de concretização de 89% leva a uma penalidade de 11% da mensalidade)	% concretização medida mensalmente.
Disponibilidade do SOC abaixo do previsto no Caderno de Encargos 99,9%, por responsabilidade imputável ao fornecedor de serviços. (excluem-se motivos de força maior)	500€ por cada ponto percentual abaixo de 99,9%	Disponibilidade medida mensalmente. A penalização, a ser aplicada, será tido em conta o acumulado anual, do seguinte modo: $(365 \text{ dias} \times 24 \text{ h}) = 8760 / 12$ (medida mensal) $730 \text{ h/mês} \times 0,999 = 729,27 \times 12 = 8751,24 \text{ h}$ (horas disponíveis anualmente).

3 - Em caso de resolução do contrato por incumprimento do prestador de serviços, a ARM, S.A. pode exigir-lhe uma pena pecuniária de até ao máximo de 20 % do respetivo preço contratual, sem prejuízo do direito de resolução sancionatória do contrato.



ÁGUAS E RESÍDUOS DA MADEIRA



4 - Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo prestador de serviços ao abrigo dos n.os 1 e 2, relativamente aos serviços cujo atraso na respetiva conclusão tenha determinado a resolução do contrato.

5 - Na determinação da gravidade do incumprimento, a ARM, S.A. tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do prestador de serviços e as consequências do incumprimento.

6 - A ARM, S.A. pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.

Cláusula 14.^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 sociedades ou grupos de sociedades dos seus subcontratados;
- c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;
- d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;
- e) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
- f) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem;
- g) Eventos que estejam ou devam estar cobertos por seguros.

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

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



ÁGUAS E RESÍDUOS DA MADEIRA



Cláusula 15.ª

Resolução por parte da ARM, S.A.

1 — Sem prejuízo de outros fundamentos de resolução previstos na lei, a ARM, S.A. 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, designadamente nos seguintes casos:

- a) Pelo atraso, total ou parcial, na implementação dos serviços objeto do contrato superior a três meses ou declaração escrita do prestador de serviços de que o atraso em determinados serviços excederá esse prazo;
- b) No caso de três ou mais violações dos termos críticos do SLA dentro de um período de 6 meses, a ARM reserva-se o direito de rescindir o contrato sem mais obrigações de pagamento;
- c) Pela inadequada execução da atividade contratada que comprometa o normal e futuro funcionamento dos sistemas informáticos da ARM,SA.

2 - O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao prestador de serviços e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pela ARM.

Cláusula 16.ª

Resolução 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 o montante que lhe seja devido esteja em dívida há mais de 6 (seis) meses.

2 - Nos casos previstos no n.º 1, o direito de resolução pode ser exercido mediante declaração enviada à ARM, S.A., que produz efeitos 30 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.

Capítulo IV

Caução e seguros

Cláusula 17.ª

Caução para garantir o cumprimento das obrigações

Não é exigível a prestação de caução, nos termos da alínea a) do n.º 2 do artigo 88.º do CCP.

Capítulo V

Resolução de litígios

Cláusula 18.ª

Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal da Comarca da Madeira, com expressa renúncia a qualquer outro.

Capítulo VI

Disposições finais

Cláusula 19.ª

Subcontratação e cessão da posição contratual

A subcontratação pelo prestador de serviços e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do artigo 318.º do Código dos Contratos Públicos.

Cláusula 20.ª

Gestor do contrato

1 — Nos termos do artigo 290ª-A do CCP, aquando da outorga do contrato, será incluído no clausulado do mesmo a designação do Gestor do Contrato nomeado pela ARM, S.A..

2 — As competências do Gestor do Contrato são as definidas no contrato (quando aplicável), bem como as definidas no CCP e no artigo 8.ª A do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto, na sua atual redação.

Cláusula 21.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 22.ª

Contagem dos prazos

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

Cláusula 23.ª

Legislação aplicável

O contrato é regulado pela legislação portuguesa.

Cláusula 24.ª

Proteção de dados

O Cocontratante obriga-se a cumprir com o enquadramento jurídico geral da Lei de Proteção de Dados existente em Portugal e o quadro jurídico especial do Regulamento Geral de Proteção de Dados (RGPD), em vigor a partir de 25 de maio de 2018, aceitando expressamente regular esta questão conforme estabelecido no Anexo III «Conformidade com o RGPD - Regulamento Geral de Proteção de Dados» a este procedimento concursal e que dele faz parte integrante.



ÁGUAS E RESÍDUOS DA MADEIRA



Cláusula 25.ª

Consulta preliminar ao mercado

- 1 — Nos termos do artigo 35.º-A do Código dos Contratos Públicos, foi realizada uma consulta preliminar ao mercado, de modo a obter informações relevantes para estabelecer, entre outras, o preço base.
- 2 — As informações obtidas foram vertidas nas especificações técnicas constantes deste caderno de encargos e foi com base naquelas que se obteve o preço base fixado no presente caderno de encargos, em conformidade com o disposto no n.º 3 do artigo 47.º do CCP.
- 3 — Toda a informação relevante resultante da consulta preliminar, caso seja solicitada, será disponibilizada aos futuros concorrentes do procedimento, o que necessariamente só ocorrerá após terminado o prazo de apresentação de propostas, salvo se os documentos que constituem a proposta forem classificados como confidenciais por parte do interessado.



ÁGUAS E RESÍDUOS DA MADEIRA



ANEXO I

CARATERÍSTICAS DO SERVIÇO A PRESTAR

Descrição	Prazo
Serviços “SOC – Security Operations Center”, nas condições definidas no anexo II do caderno de encargos	24 meses (após a implementação)

Características principais

O Serviço SOC (SOCaaS)/CSIRT pretendido pela ARM,SA inclui os seguintes pontos:

- Setup do serviço de forma a proceder a:
 - o Identificação e catalogação de ativos no âmbito, caso o número dos mesmos seja limitado;
 - o Conformação da Identificação dos ativos críticos;
 - o Levantamento às configurações dos equipamentos;
 - o Identificação e apoio na definição de medidas corretivas e processos automáticos a serem implementadas;
 - o Implementação de uma ligação independente das ligações internet existentes na ARM – Site-to-Site desde a ARM.SA até ao SOC . Esta ligação deve incluir uma Firewall dedicada ao tráfego entre a ARM e o SOC.
 - o Desenho de use-cases específicos da ARM, S.A., tanto aplicados à estrutura IT como a estrutura OT.
 - o Apoio na Implementação dos eventuais agentes nos endpoints da ARM, S.A..

Características obrigatórias da prestação dos serviços SOC / CSIRT.

- As ferramentas SIEM / SOAR - Security Orchestration Automation and Response – (ou outra(s) com funcionalidades equivalentes) a utilizar devem:
 - o Ter o licenciamento completamente a cargo do fornecedor de serviços.
 - o Estar instaladas em Datacenter do fornecedor de serviços ou por este contratado e em território da União Europeia.
 - o Não ter limite de eventos nem de tráfego a ingerir.
 - o Implementar automatismos de remediação.
 - Nos endpoints com agente (ou por outro meio) – Ex: Isolar um endpoint, permitindo no entanto a conexão para investigação.
 - Nos Firewalls
 - No Active Directory
 - o Retenção de logs no mínimo por 12 meses.



ÁGUAS E RESÍDUOS DA MADEIRA



- Âmbito da recolha de logs:
 - o EndPoints com SO Windows +- 600
 - o Eventos em sistemas não Windows (ex: Linux) +- 20
 - o Citrix , Parallels.
 - o Eventos de rede (firewall, switching, routing, VPN,...) +-12
 - o IP Phones - 360 – 1 x Cisco Call Manager
 - o Impressoras +- 35 – 1 x Canon UFlow
 - o Fortimail Cloud
 - o Cisco DUO Security
 - o Cortex XDR
 - o Eventos Aplicacionais (Ex: Veeam, MS Dynamics, MS SQL, Oracle, IIS, MS Exchange)
 - o Eventos de sistemas SCADA.
 - o Eventos Sistemas Cloud (cisco umbrella, azure, Aws, etc)

NOTA1: No decurso da prestação de serviços podem ser alteradas as fontes de informação. A ingestão de logs dessas fontes será previamente acordada com o prestador de serviços.

NOTA 2 : (TOTAL DE ATIVOS MINIMO A CONSIDERAR) – 750 aos quais de deve acrescentar uma margem de crescimento de 10% gradual ao longo de 24 meses.

- Integração com sistemas Threat Intelligence, sem limite de sessões.
- Implementar User and Entity Behavior Analytics (UEBA)
- Implementar NTA.
- Enquadrar eventos na matriz MITRE ATT&CK .
- Monitorização deve abranger áreas OT da ARM, S.A. equipadas com sistemas SCADA.
- Gestão de Vulnerabilidades:
 - o Deve abranger pelo menos 250 ativos (a identificar em fase de projeto)
 - o Deve abranger, para além dos sistemas operativos dos ativos identificados, todo o software conhecido que esteja instalado no endpoint.

Características do serviço – O Serviço terá de ter implementados pelo menos os seguintes processos:

- Monitorização, Detecção e Resposta a incidentes de segurança em regime de 24x7x365;
- Análise dos eventos de segurança para confirmar se constituem um incidente de cibersegurança;
- Comunicar proactivamente ameaças de segurança / alertas de cibersegurança;



ÁGUAS E RESÍDUOS DA MADEIRA



- o Utilizando plataforma de ticketing de modo automatizado.
- o Por email ou telefone em casos justificados.
- Investigar ameaças emergentes sempre que solicitado pela ARM, e/ou de forma pro-ativa (ex: outbreaks, ataques ao setor específico das utilities)
- Gestão de vulnerabilidades (análise e propostas de eliminação e/ou melhoria dos sistemas)
- Correlação dos eventos de segurança com indicadores externos; (ex: integração com sistemas Threat Intelligence)
- Receção e triagem dos eventos de segurança, de acordo com processo de resposta a incidentes de cibersegurança da ARM, S.A.
- Classificar e categorizar os incidentes de cibersegurança;
- Apoiar as equipas da ARM na resposta a incidentes de cibersegurança ao nível da contenção, erradicação, recuperação e investigação; incluindo no contacto com o CNCS
- Assegurar que a erradicação e prevenção são efetivas, mediante relatório pormenorizado das ações efetuadas e seu resultado.
- Registar os incidentes de cibersegurança, efetuando a documentação das ações efetuadas no tratamento do mesmo e apoiando as diferentes equipas operacionais da ARM na obtenção de dados relevantes;
- Atualização/ Criação de novas regras de deteção de eventos de segurança (use-cases) , em tempo real ajustadas à realidade da ARM, S.A..
- A disponibilidade do serviço SOC deve ser de 99,9%.
- No final do contrato, os logs ingeridos e mantidos devem poder ser exportados em formato syslog (ou outro reconhecidamente standard) e entregues a ARM, S.A..

Equipa de prestação do serviço:

Para a execução das especificações técnicas do presente procedimento a **equipa técnica** responsável pela execução das prestações objeto do contrato a celebrar deve cumprir as seguintes **exigências**:

- Deve operar em Território da União Europeia e expressar-se em português.
- Deve ser composta por pelo menos 5 elementos, sendo 1 deles gestor da equipa, que devem possuir:
 - o Elemento Gestor / Coordenador da equipa prestadora dos serviços - experiência mínima de 8 anos na área de Cibersegurança.
 - o Elementos da equipa prestadora de serviços - experiência mínima de 3 anos por elemento na área de Cibersegurança.
 - o Pelo menos 5 dos elementos da equipa têm que ter **individualmente, pelo menos, uma das certificações de cibersegurança exigidas no programa de procedimento.**



ÁGUAS E RESÍDUOS DA MADEIRA



- o Cumulativamente, a equipa deverá possuir, no mínimo, 6 das certificações de cibersegurança exigidas no programa de procedimento.
- o O gestor indicado deverá possuir, no mínimo, uma das certificações exigidas.

Monitorização do Serviço

- SIEM/SOAR (*ou outra(s) com funcionalidades equivalentes*) com monitorização e análise de logs; O prestador de serviços deve proporcionar à equipa da ARM o acesso a dashboards em tempo real, que incluam no mínimo:
 - o Alertas de eventos ocorridos na rede.
 - o Vulnerabilidades encontradas
 - o Tráfego na rede interno e externo.
 - o Acessos aos ativos críticos.
 - o Informação sobre user behaviour.
- Relatórios mensais do serviço (pelo menos).
 - o Vulnerabilidades encontradas com sugestão de eliminação/mitigação.
 - o Alertas de segurança e seu tratamento
 - o Outbreaks, em particular que afetem (afetaram) organizações do tipo da ARM.
 - o Estatísticas de tráfego na rede.
- Trimestralmente
 - o Reunião de avaliação do serviço em que deve estar presente o gestor de equipa de prestação dos serviços.
- Anualmente
 - o Relatório inventário de ativos com a informação necessária ao cumprimento do DL65/2021.
 - o Relatório de Incidentes, com o formato e informação necessária ao cumprimento do DL65/2021.
- Manutenção de inventario de ativos na plataforma SIEM (ou outra).



ÁGUAS E RESÍDUOS DA MADEIRA



SLA

O prestador de serviços deve comprometer-se com o seguinte SLA:

	Gestão de Incidentes de Segurança		Incidente de Segurança
Severidade	Tempo Primeira Notificação ao cliente	% Concretização mínima	Relatório após incidente
Crítica	30 minutos	90%	2 Dias Úteis Seguintes
Elevada	90 Minutos	90%	2 Dias Úteis Seguintes
Moderada	120 Minutos	90%	Apenas para incidências repetitivas
Baixa	12 horas	90%	Apenas para incidências repetitivas

Tabela 1 Criticidades

Tipo	Impacto	Urgência
Alta	Afetação severa de serviços críticos. Número elevado de utilizadores/clientes com impacto sério. Informação estratégica comprometida (confidencialidade, integridade, disponibilidade). Alto impacto económico. Alto impacto em reputação	Rápida velocidade de expansão. Área de negócio crítica em caso de indisponibilidade de serviço. Risco de se converter em um incidente crítico se não se atuar de forma rápida. Requisitos legais exigem uma resposta imediata.
Média	Afetação parcial de serviços críticos Número moderado de utilizadores/clientes com impacto. Informação não estratégica comprometida (confidencialidade, integridade, disponibilidade) Impacto económico médio Impacto moderado na reputação	Velocidade moderada de expansão dos danos Unidade de negócio crítica afetada sem risco de indisponibilidade de serviço Utilizadores VIP afetados.
Baixa	Degradação leve nos serviços críticos ou impacto em serviços não críticos. Número reduzido e controlado de utilizadores/clientes com degradação de serviço Não há Informação comprometida (confidencialidade, integridade, disponibilidade) Impacto económico baixo. Impacto mínimo na reputação	Velocidade baixa de expansão dos danos Áreas de negócio não críticas afetadas



ÁGUAS E RESÍDUOS DA MADEIRA



Tabela 2 Definição da Severidade

Severidade		Urgência		
		Alta	Média	Baixa
Impacto	Alta	Crítica	Elevada	Moderada
	Média	Elevado	Moderada	Baixa
	Baixa	Moderada	Baixa	Baixa



ÁGUAS E RESÍDUOS DA MADEIRA



TABELAS DE CARACTERÍSTICAS TÉCNICAS:

1 ESPECIFICAÇÕES TÉCNICAS

(Só são aplicáveis à execução contratual, as especificações a que o adjudicatário se tenha vinculado na sua proposta)

Num.	Característica
1	Número de ativos ilimitado
2	Gestão de vulnerabilidades na totalidade dos ativos monitorizados.
3	<i>SIEM/SOAR a utilizar figura no mais recente Quadrante Gartner para sistema SIEM/SOAR</i>
4	Leader ou challenger
5	Niche Player ou visionaire
6	Inclui gestão do sistema Cortex XDR instalado na ARM, S.A.
7	Inclui instalação de “honeypots”
8	Inclui ações de ciber-educação (ex: possibilidade de campanhas phishing e educação users)
9	Ações de contenção não automáticas - O prestador de serviços intervém nos sistemas de ARM (a combinar) e efetua os processos manuais necessários para a contenção num incidente.
10	<i>Inclui Testes de Penetração (pelo menos 6 interações anuais)</i>
11	Por equipa do prestador de Serviços
12	Por equipa externa ao prestador de serviços
13	Inclui análise forense (pelo menos 2 análises anuais)



ÁGUAS E RESÍDUOS DA MADEIRA



2 ESPECIFICAÇÕES TÉCNICAS – EQUIPA DE TRABALHO

(São aplicáveis as certificações da equipa de trabalho indicadas na proposta do adjudicatário)

Num.	Característica
14	Certificações Cibersegurança apresentadas pelos elementos da equipa prestadora do serviço.
15	CISSP – Certified Information Systems Security Professional
16	CISM – Certified Information Security Manager;
17	(CISA) Certified Information Systems Auditor
18	GIAC Security Operations Manager
19	CEH - Certified Ethical Hacker
20	CompTIA Security+
21	CompTIA CySA+
22	ISO IEC 27001 Certification
23	GCIH-Certified Incident Handler
24	CSA – Certified SOC Analyst
25	Information Security Foundation (ISFS) – EXIN
26	CND – Certified Network Defender
27	OSCP – Offensive Security Certified Professional
28	GCFA - SANS FOR508 - Advanced Incident Response, Threat Hunting and Digital Forensics
29	CHFI - Computer Hacking Forensic Investigator
30	GCIA -Network Intrusion Analyst
31	GIAC Certified Forensic Analyst;
32	CHFI - Computer Hacking Forensic Investigator
33	CompTIA Pentest+
34	IAAP Certified Information Privacy Professional / Europe (CIPP/E)
35	Certificações de fabricantes (detidas pelos elementos da equipa prestadora do Serviço)
36	Fortinet – Certified Professional – ou equivalente
37	Palo Alto – Certified Network Security Analyst ou equivalente
38	Cisco – CCPNP Security – ou equivalente



ÁGUAS E RESÍDUOS DA MADEIRA



ESPECIFICAÇÃO DAS CARACTERÍSTICAS TÉCNICAS

Num.	Característica	Especificação
1	Número de ativos Ilimitado	O Serviço não limita o número de ativos “vivos” que monitoriza.
2	Gestão de Vulnerabilidades em todos os ativos monitorizados	O serviço não limita o número de ativos sobre o qual é efetuada a gestão de vulnerabilidades, aplicando a mesma ao universo dos ativos monitorizados.
3	<i>SIEM/SOAR a utilizar figura no último Quadrante Gartner para sistema SIEM</i>	O SIEM/SOAR e Utilizar figura no último “magic quadrandt” da Gartner em posição Niche Player ou visionaire, ou em posição Leader ou Challenger.
6	Inclui gestão do sistema Cortex XDR instalado na ARM,SA	Serviços para gestão do sistema Palo Alto Cortex XDR, instalado em cerca de 500 endpoint da ARM,SA. Deve incluir: <ul style="list-style-type: none">- Definição de automatismos- Desenho de dashboards.- Monitorização do sistema.
7	Inclui instalação de “honeypots”	“Honeypots” para tentar enganar o atacante, ganhando tempo para se conseguir perceber o objetivo e progressão do ataque e mapear o padrão.
8	Inclui ações de ciber-educação (ex: possibilidade de campanhas phishing e educação users)	
9	Ações de contenção e erradicação não automáticas - O prestador de serviços intervém nos sistemas de ARM (a combinar) e efetua os processos manuais necessários para a contenção e erradicação num incidente.	De modo não automático o prestador de serviços intervém nos sistemas da ARM, S.A. (a combinar), e implementa ações de contenção e erradicação de um possível incidente. Intervindo, designadamente no âmbito dos sistemas: Rede (incluindo Fortigate, Cisco Meraki e Cisco Switchs), Cortex XDR e Active Directory (Windows 2022) , que podem vir a ser outros, caso existam alterações na arquitetura informática da ARM.
10	<i>Testes de Penetração</i>	O serviço inclui testes de penetração nos sistemas da ARM (de modo não disruptivo), no mínimo com equipas “Purple Team” (Red vs Blue)



ÁGUAS E RESÍDUOS DA MADEIRA



Num.	Característica	Especificação
13	Inclui análise forense (pelo menos 2 análises anuais)	Inclusão de pelo menos 2 eventos de análise forense anuais, e a efetuar durante a vigência do contrato.
15 a 34	<i>Certificações Cibersegurança apresentadas pelos elementos equipa prestadora do serviço.</i>	Certificações relativas a segurança de informação e Cibersegurança.
36 a 38	<i>Certificações de fabricantes</i>	Certificações de fabricantes na área da Cibersegurança, equivalentes ou superiores às indicadas na tabela (n.ºs 36,37 e 38), sempre que sejam reconhecidas pelo respetivo fabricante.

ANEXO III

«Conformidade com o RGPD - Regulamento Geral de Proteção de Dados»

Introdução.

Definições no quadro do RGPD e da LPDP

1. NORMA DE PROTEÇÃO DE DADOS PESSOAIS

Toda e qualquer norma jurídica aplicável no âmbito da proteção de dados pessoais e da segurança da informação pessoal, seja de carácter internacional ou comunitário, seja de carácter nacional, tal como, designadamente, o Regulamento Geral sobre a Proteção de Dados, a Lei de Proteção de Dados Pessoais e outra Legislação Complementar vigente no ordenamento jurídico.

2. RESPONSÁVEL PELO TRATAMENTO

«Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

3. SUBCONTRATANTE

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

Cláusula 1ª

(Conformidade com a NORMA DE PROTEÇÃO DE DADOS PESSOAIS)

1. Cada uma das Partes deve atuar em conformidade com todas as normas vigentes no ordenamento jurídico nacional em matéria de proteção de dados pessoais e de segurança da informação, normas essas designadas doravante por NORMA DE PROTEÇÃO DE DADOS PESSOAIS, cumprindo com as respetivas obrigações.
2. A NORMA DE PROTEÇÃO DE DADOS PESSOAIS abrange todo e qualquer tipo de norma vigente e aplicável no ordenamento jurídico nacional bem como toda e qualquer interpretação ou decisão de uma entidade administrativa ou jurisdicional nas referidas matérias e toda e qualquer recomendação, código de conduta ou mecanismo de certificação vigente e aplicável emitido por uma autoridade de supervisão.

Cláusula 2ª

(Responsável pelo tratamento e subcontratante)

No âmbito do Contrato celebrado entre a ARM - Águas e Resíduos da Madeira, S.A. e o Cocontratante, ambas as partes acordam que, em matérias de proteção de dados pessoais e de segurança da informação, a ARM - Águas e Resíduos da Madeira, S.A. será a entidade responsável pelo tratamento e o Cocontratante será o SUBCONTRATANTE, de acordo com as definições e os termos gerais constantes da NORMA DE PROTEÇÃO DE DADOS PESSOAIS.

Cláusula 3ª

(Medidas técnicas e organizativas)

O SUBCONTRATANTE deve implementar e executar as medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos da NORMA DE PROTEÇÃO DE DADOS PESSOAIS, assegurando a defesa dos direitos do titular dos dados e assumindo os custos pela implementação dessas medidas, como partes integrantes dos serviços objeto do Contrato.

Cláusula 4ª

(Sub-subcontratação)

1. O SUBCONTRATANTE não está autorizado a contratar outro subcontratante sem que a responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral.
2. Existindo uma autorização geral por escrito, o SUBCONTRATANTE deve informar a responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim à responsável pelo tratamento a oportunidade de se opor a tais alterações.
3. Se o SUBCONTRATANTE contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta da responsável pelo tratamento, são impostas a esse outro subcontratante, por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, as mesmas obrigações em matéria de proteção de dados que as estabelecidas neste Anexo Único, devendo obter garantias por parte deste de que cumprirá as obrigações da NORMA DE PROTEÇÃO DE DADOS PESSOAIS.
4. Se o SUBCONTRATANTE contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta da responsável pelo tratamento, e se esse outro subcontratante não cumprir as suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante.
5. Se o SUBCONTRATANTE contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, o contrato deve ser feito por escrito, incluindo em formato eletrónico.

Cláusula 5ª

(Termos de vinculação)

O tratamento de dados pessoais no âmbito das relações de subcontratação entre as partes é regulado por este Anexo Único.

Cláusula 6ª

(Circulação e transferência de dados pessoais)

O SUBCONTRATANTE não está autorizado, sem que a responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral e, neste caso, cumpridas que sejam as respetivas instruções, a proceder à transferência de dados pessoais para entidades terceiras, incluindo no



ÁGUAS E RESÍDUOS DA MADEIRA



que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso a responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público.

Cláusula 7ª

(Compromisso de confidencialidade)

O SUBCONTRATANTE deve assegurar que os colaboradores, trabalhadores ou pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

Cláusula 8ª

(Medidas de segurança)

1. O SUBCONTRATANTE deve adotar todas as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares.
2. Entre outras, o SUBCONTRATANTE deve aplicar as seguintes medidas, consoante o que for adequado:
 - a) medidas de pseudonimização e de cifragem dos dados pessoais;
 - b) medidas para assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
 - c) medidas para restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
 - d) processos para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.
3. O SUBCONTRATANTE deve proceder à avaliação da adequação do nível de segurança, devendo ter em conta, designadamente, os riscos apresentados pelo tratamento de dados que esteja a realizar.
4. O SUBCONTRATANTE deve proceder à implementação de todas as medidas necessárias para prevenir a destruição, perda e alteração acidentais ou ilícitas, a divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento no âmbito deste contrato.

Cláusula 9ª

(Conformidade dos colaboradores ou trabalhadores)

1. O SUBCONTRATANTE é responsável por garantir a conformidade da atividade de todos os seus colaboradores ou trabalhadores com a NORMA DE PROTEÇÃO DE DADOS PESSOAIS.
2. O SUBCONTRATANTE deve garantir a implementação das medidas de segurança necessárias à respetiva conformidade, estando obrigado a celebrar acordos de confidencialidade enquadrados em contratos escritos com esses colaboradores ou trabalhadores.
3. Sempre que seja necessário para a realização de operações de tratamento de dados pessoais inerentes ao Contrato, o SUBCONTRATANTE garante o consentimento, nos termos da NORMA DE PROTEÇÃO DE DADOS PESSOAIS, de todos os seus colaboradores ou trabalhadores.



ÁGUAS E RESÍDUOS DA MADEIRA



4. O SUBCONTRATANTE deve adotar as medidas consideradas adequadas para garantir a fiabilidade do tratamento dos dados pessoais pelos seus colaboradores e trabalhadores, sendo responsável em proceder à formação adequada destes para garantia da atividade em conformidade com a NORMA DE PROTEÇÃO DE DADOS PESSOAIS.

Cláusula 10ª

(Assistência à responsável pelo tratamento)

1. Assistência na resposta ao exercício dos direitos dos titulares:

Tendo em conta a natureza do tratamento, o SUBCONTRATANTE presta assistência à responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que esta cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos em matéria de proteção de dados pessoais previstos na NORMA DE PROTEÇÃO DE DADOS PESSOAIS, registando e notificando à responsável pelo tratamento, no prazo de dois dias úteis, quer todos os pedidos dos titulares dos dados pessoais, quer as reclamações ou quaisquer outros pedidos relacionados com as obrigações das partes em matéria de conformidade com a NORMA DE PROTEÇÃO DE DADOS PESSOAIS.

2. Assistência nas notificações ou comunicações de violação de incidentes de dados pessoais:

Tendo em conta a natureza do tratamento e a informação que tem ao seu dispor, o SUBCONTRATANTE deve prestar assistência à responsável pelo tratamento no sentido de esta assegurar o cumprimento das obrigações previstas na NORMA DE PROTEÇÃO DE DADOS PESSOAIS em matéria de notificações ou comunicações de violação de dados pessoais.

3. Assistência na realização de avaliações de impacto:

Tendo em conta a natureza do tratamento e a informação que tem ao seu dispor, o SUBCONTRATANTE deve prestar assistência à responsável pelo tratamento no sentido de esta assegurar o cumprimento das obrigações previstas na NORMA DE PROTEÇÃO DE DADOS PESSOAIS em matéria de realização de avaliações de impacto das operações de tratamento previstas sobre a proteção de dados pessoais.

4. Assistência na realização de consultas prévias:

Tendo em conta a natureza do tratamento e a informação que tem ao seu dispor, o SUBCONTRATANTE deve prestar assistência à responsável pelo tratamento no sentido de esta assegurar o cumprimento das obrigações previstas na NORMA DE PROTEÇÃO DE DADOS PESSOAIS em matéria de consultas prévias às autoridades de supervisão.

Cláusula 11ª

(Conservação dos dados)

1. O SUBCONTRATANTE deve cumprir com os prazos exigidos pela NORMA DE PROTEÇÃO DE DADOS PESSOAIS para conservação dos dados pessoais, devendo seguir as instruções gerais ou especiais da responsável pelo tratamento nessa matéria.
2. Consoante a escolha da responsável pelo tratamento, o SUBCONTRATANTE deve apagar ou devolver-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros.



ÁGUAS E RESÍDUOS DA MADEIRA



Cláusula 12ª

(Dever de prestar informações)

1. O SUBCONTRATANTE deve disponibilizar à responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na NORMA DE PROTEÇÃO DE DADOS PESSOAIS em matéria de proteção de dados pessoais e de segurança da informação.
2. Em especial, o SUBCONTRATANTE deve informar imediatamente a responsável pelo tratamento se, no seu entender, alguma instrução violar o Contrato ou este Anexo Único ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados.

Cláusula 13ª

(Auditorias e inspeções)

O SUBCONTRATANTE deve permitir ou facilitar todas as auditorias ou inspeções, conduzidas pela responsável pelo tratamento ou por outro auditor por esta mandatado, que sejam consideradas necessárias no âmbito do Contrato, assumindo a responsabilidade pelo pagamento dos custos acrescidos associados a essas auditorias ou inspeções sempre que sejam detetadas desconformidades da sua exclusiva responsabilidade.

Cláusula 14ª

(Tratamento sob a autoridade da responsável pelo tratamento)

O SUBCONTRATANTE ou qualquer pessoa que, agindo sob a sua autoridade, tenha acesso a dados pessoais, não procede ao tratamento desses dados exceto por instrução da responsável pelo tratamento, salvo se a tal for obrigado por força do direito da União ou dos Estados-Membros.

Cláusula 15ª

(Registos das atividades de tratamento)

1. O SUBCONTRATANTE e, sendo caso disso, os seus representantes ou subcontratantes, deve conservar um registo de todas as categorias de atividades de tratamento realizadas em nome e por conta da responsável pelo tratamento.
2. Deste registo deverá constar:
 - a) O nome e contactos do SUBCONTRATANTE ou subcontratantes, bem como, sendo caso disso do representante da responsável pelo tratamento ou do subcontratante e do encarregado da proteção de dados;
 - b) As categorias de tratamentos de dados pessoais efetuados em nome de cada responsável pelo tratamento;
 - c) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, do RGPD, a documentação que comprove a existência das garantias adequadas;
 - d) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1, do RGPD.
3. O registo é efetuado por escrito, incluindo em formato eletrónico.



ÁGUAS E RESÍDUOS DA MADEIRA



4. O SUBCONTRATANTE e, caso existam, os seus subcontratantes, devem disponibilizar, a pedido, o registo à responsável pelo tratamento bem com à autoridade de controlo nos termos da NORMA DE PROTEÇÃO DE DADOS PESSOAIS.

Cláusula 16ª

(Dever de cooperação)

O SUBCONTRATANTE deve cooperar com a responsável pelo tratamento sempre que haja necessidade de proceder a respostas aos pedidos da autoridade de controlo, no âmbito da prossecução das suas atribuições.

Cláusula 17ª

(Dever de notificação de uma violação de dados pessoais)

1. O SUBCONTRATANTE deve implementar um sistema de gestão de incidentes em matéria de dados pessoais e de segurança da informação.
2. Em caso de violação de dados pessoais, o SUBCONTRATANTE deve notificar desse facto a responsável pelo tratamento, sem demora injustificada e, sempre que possível, até 12 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.
3. Se a notificação não for transmitida no prazo de 12 horas, deve ser acompanhada dos motivos do atraso.
4. A notificação referida deve, pelo menos:
 - a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
 - b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;
 - c) Descrever as consequências prováveis da violação de dados pessoais;
 - d) Descrever as medidas adotadas ou propostas pelo SUBCONTRATANTE para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;
5. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada.
6. O SUBCONTRATANTE deve documentar quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada, disponibilizando essa documentação à responsável pelo tratamento.

Cláusula 18ª

(Responsabilidade e indemnizações)

O SUBCONTRATANTE deve indemnizar a responsável pelo tratamento por quaisquer danos causados resultantes de dados pessoais, pela sua atuação ou pela atuação de um qualquer seu subcontratado, quer esses danos sejam decorrentes da violação dos termos deste contrato, quer esses danos sejam decorrentes da violação dos termos da NORMA DE PROTEÇÃO DE DADOS PESSOAIS.

Cláusula 19ª

(Gabinete de Proteção de Dados)

Para o exercício de qualquer tipo de direitos de proteção de dados e de privacidade ou para qualquer assunto referente aos temas da proteção de dados, privacidade e segurança da informação, o SUBCONTRATANTE pode entrar em contacto com o Gabinete de Proteção de Dados através do correio eletrónico [protecaodedados@arm.pt], descrevendo o assunto do pedido e indicando um endereço de correio eletrónico, um endereço de contacto telefónico ou um endereço de correspondência para resposta.

O Gabinete de Proteção de Dados do SUBCONTRATANTE pode ser contactado através do correio eletrónico a disponibilizar à ARM – Águas e Resíduos da Madeira, S.A.

Para além destas condições gerais, são aplicáveis todas as medidas que estão previstas no Contrato ou em outros instrumentos contratuais celebrados entre as partes para efeitos de tratamento de dados pessoais.