



CADERNO DE ENCARGOS

**PROCEDIMENTO PRÉ-CONTRATUAL DE AJUSTE DIRETO, SEGUNDO O
REGIME GERAL, PARA A “PRESTAÇÃO DE SERVIÇOS DE ASSESSORIA PARA
CONFORMIDADE AO REGIME JURÍDICO DA SEGURANÇA DO
CIBERESPAÇO”**

PROCEDIMENTO N.º ADG/09/2022

JUNHO DE 2022

CADERNO DE ENCARGOS

PRESTAÇÃO DE SERVIÇOS DE ASSESSORIA PARA CONFORMIDADE AO REGIME JURÍDICO DA SEGURANÇA DO
CIBERESPAÇO – ADG/09/2022

Índice

Capítulo I Cláusulas Gerais	4
Cláusula 1.ª Objeto contratual	4
Cláusula 2.ª Contraente público.....	4
Cláusula 3.ª Contrato	4
Cláusula 4.ª Prazo de execução e vigência	5
Cláusula 5.ª Conformidade e operacionalidade dos serviços	6
Cláusula 6.ª Local da prestação de serviços	6
Cláusula 7.ª Preço Base	7
Cláusula 8.ª Condições de pagamento.....	7
Cláusula 9.ª Avaliação de desempenho do Contraente Privado.....	9
Cláusula 10.ª Código de Conduta para Fornecedores e Subcontratados da Porto Ambiente	12
Cláusula 11.ª Requisitos Sustentáveis.....	12
Cláusula 12.ª Obrigações e deveres do Contraente Privado	13
Cláusula 13.ª Obrigações principais da Porto Ambiente.....	15
Cláusula 14.ª Acompanhamento da execução do contrato	16
Cláusula 15.ª Gestor do Contrato	16
Cláusula 16.ª Alterações ao contrato.....	16
Cláusula 17.ª Cessão da posição contratual e Subcontratação	17
Cláusula 18.ª Patentes, Licenças e marcas registadas	17
Cláusula 19.ª Confidencialidade e Proteção de dados pessoais.....	18
Cláusula 20.ª Sigilo	20
Cláusula 21.ª Causas de Força Maior	21
Cláusula 22.ª Sanções contratuais.....	22
Cláusula 23.ª Resolução do contrato pela Porto Ambiente.....	24
Cláusula 24.ª Comunicações e notificações	24
Cláusula 25.ª Contagem dos prazos	25
Cláusula 26.ª Foro competente	25

Cláusula 27.ª	Legislação aplicável.....	25
Capítulo II	Cláusulas técnicas.....	26
Cláusula 28.ª	Âmbito de aplicação.....	26
Cláusula 29.ª	Atividades para avaliação do Sistema de Gestão de Segurança da Informação.....	26
Cláusula 30.ª	Atividades Técnicas	27
Cláusula 31.ª	Análises Técnicas.....	29
Cláusula 32.ª	Descrição das Atividades Técnicas para resposta a incidentes de segurança 31	
Cláusula 33.ª	Descrição das Atividades Processuais.....	34
Cláusula 34.ª	Descrição das Atividades de Desenvolvimento da arquitetura de segurança 37	
Cláusula 35.ª	Descrição das Atividades de Implementação.....	39
Cláusula 36.ª	Descrição de Capacidades.....	40
Cláusula 37.ª	Descrição de Capacidades Avançadas.....	44
Cláusula 38.ª	Capacidades de Resposta a Incidentes de Segurança	44
Cláusula 39.ª	Análise de Vulnerabilidades e Integração com o SOC	47
Cláusula 40.ª	Funcionalidade e Benefício	49
Cláusula 41.ª	Formação aos colaboradores	50
Cláusula 42.ª	Plano de Monitorização.....	52
Cláusula 43.ª	Outros Deveres do Contraente Privado.....	53

CAPÍTULO I

CLÁUSULAS GERAIS

Cláusula 1.ª

Objeto contratual

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual de Ajuste Direto, segundo o Regime Geral, que tem por fundamento o previsto nas disposições conjugadas dos artigos 16.º, n.ºs 1, alínea a) e 2, alínea e), 20.º, n.º 1, alínea d) e 112.º a 127.º, todos do Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, doravante abreviadamente designado por CCP, e por objeto principal a “Prestação de Serviços de Assessoria para conformidade ao Regime Jurídico da Segurança do Ciberespaço”, cujas características se encontram melhor identificadas no Capítulo II do presente Caderno de Encargos relativo às Cláusulas Técnicas.

Cláusula 2.ª

Contraente público

O contraente público é a Empresa Municipal de Ambiente do Porto, E.M., S.A. (doravante abreviadamente designada por Porto Ambiente), sita na Praça General Humberto Delgado, 4049-001 Porto, tendo sido a decisão de contratar tomada pelo Conselho de Administração da Porto Ambiente, ao abrigo do disposto no n.º 1 do artigo 36.º do CCP, na sua reunião ordinária do dia 22 de junho de 2022.

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) Caso se verifiquem, os suprimientos dos erros e das omissões do Caderno de Encargos identificados pela entidade convidada, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b) Caso se verifiquem, os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c) O presente Caderno de Encargos;
 - d) A proposta adjudicada;
 - e) Caso se verifiquem, os esclarecimentos sobre a proposta adjudicada prestados pelo Contraente Privado.
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 CCP e aceites pelo Contraente Privado nos termos do disposto no artigo 101.º desse mesmo diploma legal.
5. Salvo nos casos previstos no artigo 95.º do CCP, o contrato deve ser reduzido a escrito através da elaboração de um clausulado em suporte informático com a aposição de assinaturas eletrónicas.

Cláusula 4.ª

Prazo de execução e vigência

- 1. O Contraente Privado obriga-se a executar o Contrato nos termos exigidos pelo presente Caderno de Encargos, pelo prazo máximo de 12 (doze) meses.
- 2. A execução do Contrato terá início na data da sua outorga.
- 3. Caso o preço global fixado seja atingido antes de decorrido o prazo de

duração do Contrato, tal situação implicará a imediata cessação do mesmo, sem que o Contraente Privado tenha direito a qualquer indemnização ou compensação, a qualquer título.

Cláusula 5.ª

Conformidade e operacionalidade dos serviços

1. O Contraente Privado obriga-se a prestar à Porto Ambiente os serviços objeto do Contrato com as características e requisitos previstos nas especificações técnicas constantes do presente Caderno de Encargos.
2. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens objeto da presente prestação de serviços.
3. O Contraente Privado fica sujeito, com as devidas adaptações e no que se refere aos elementos entregues ao Contraente Público em execução do contrato, às exigências legais, obrigações e prazos aplicáveis e garantia de assistência técnica, nos termos do Código dos Contratos Públicos e demais legislação aplicável.
4. O Contraente Privado é responsável perante a Porto Ambiente por qualquer defeito ou discrepância dos elementos previstos no âmbito da prestação de serviços do contrato que existam quando os mesmos lhe forem entregues.

Cláusula 6.ª

Local da prestação de serviços

1. Os serviços serão prestados nas instalações da Porto Ambiente ou do Contraente Privado, dependendo da natureza das tarefas, conforme acordado entre as partes.
2. Para os efeitos do número anterior, as instalações da Porto Ambiente situam-se na Rua de S. Dinis, n.º 249, 4250-434 Porto, ou na Rua de Acácio Lino, n.º 101, 4250-013 Porto, conforme indicado por esta.

3. Todos os serviços H-SOC do Contraente Privado são prestados em modo remoto.

Cláusula 7.ª

Preço Base

1. O preço que serve como parâmetro base do preço contratual é de 16.200,00€ (dezasseis mil e duzentos euros), sendo este o preço máximo que a Porto Ambiente se dispõe a pagar pela execução de todas as prestações que constituem o objeto do presente procedimento pré-contratual, não incluindo o IVA à taxa legal aplicável (23%).
2. O preço base deverá atender aos pressupostos atinentes ao prazo de execução e de vigência do contrato, de acordo com o disposto na Cláusula 4.ª.
3. O preço a apresentar tem de incluir todos os custos, despesas ou encargos associados ao objeto contratual cuja responsabilidade não seja expressamente atribuída à Porto Ambiente, designadamente as despesas de alojamento, alimentação ou deslocação de pessoal do Contraente Privado, bem como despesas de aquisição, transporte, armazenamento e manutenção de meios que o mesmo afete à execução do contrato.
4. O preço a apresentar inclui, também, custos tecnológicos e serviços profissionais de instalação, configuração e operação das ferramentas do projeto associado à prestação de serviços.

Cláusula 8.ª

Condições de pagamento

1. Pela realização das prestações objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a Porto Ambiente pagará ao Contraente Privado o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido, com arredondamento às centésimas.

2. As quantias devidas pela Porto Ambiente devem ser pagas no prazo de 30 dias após a receção das respetivas faturas, emitidas nos termos do artigo 36.º do CIVA, após o vencimento da obrigação respetiva e a efetiva realização das prestações objeto do contrato, devendo ainda cumprir as regras supletivas consagradas no artigo 9.º, n.º 1, da Lei n.º 8/2012, de 21 de fevereiro, na sua redação atual.
3. Em caso de discordância por parte da Porto Ambiente quanto aos valores indicados nas faturas, deve esta comunicar ao Contraente Privado, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.
4. Em caso de atraso da Porto Ambiente no cumprimento do prazo de pagamento, são devidos juros de mora sobre o montante em dívida à taxa legalmente fixada para o efeito pelo período correspondente à mora, sem prejuízo do direito de resolução do Contraente Privado.
5. As faturas serão enviadas pelo Contraente Privado à Porto Ambiente, preferencialmente para o endereço eletrónico faturas@portoambiente.pt, ou remetidas para o endereço postal sito na Rua de São Dinis, n.º 249, 4250-434 Porto.
6. O Contraente Privado deverá emitir fatura eletrónica, nos termos do disposto no artigo 299.º-B do CCP, a qual fará obrigatoriamente menção ao número de requisição e ao número de compromisso constante do Contrato.
7. A importância dos pagamentos a receber pelo Contraente Privado será o produto da multiplicação dos preços unitários pela quantidade de trabalhos efetivamente executados.
8. Desde que devidamente emitidas e observado o disposto nos números 2, 5 e 6 da presente cláusula, as faturas serão pagas através de transferência bancária.

Cláusula 9.ª

Avaliação de desempenho do Contraente Privado

1. O Contraente Privado será objeto de avaliação de desempenho no decurso da execução do contrato.
2. O resultado da avaliação de desempenho será divulgado anualmente junto do Contraente Privado.
3. Os critérios de avaliação são os seguintes:

- i. *Qualidade (Q)* – avalia a conformidade do bem/serviço com os requisitos aplicáveis no momento de receção do bem ou da conclusão da realização do serviço, ou num momento posterior em que possam vir a manifestar-se eventuais falhas:

100% a 86%	Bem/serviço sempre conforme ou pontuais não conformidades menores (prontamente corrigidas ou sem consequências significativas no desempenho)
85% a 71%	Não conformidades maiores de carácter pontual (com consequências significativas no desempenho), ou menores, mas frequentes
70% a 0%	Ocorrência de diversas não conformidades maiores

- ii. *Prazo (P)*- avalia a adequabilidade dos prazos praticados e/ou o grau de cumprimento de prazos estabelecidos ou acordados:

100% a 86%	Prazos adequados e cumprimento sistemático dos prazos acordados ou prazos razoáveis/ocorrência <u>pontual</u> de atrasos <u>sem consequências</u> significativas no desempenho
85% a 71%	Prazos razoáveis/ocorrência <u>pontual</u> de atrasos <u>com consequências</u> significativas no desempenho
70% a 0%	Ocorrência frequente de atrasos na entrega

- iii. *Critério Procedimento de Compra*:

Cumprimento Requisitos Compras (Admt) - avalia o cumprimento da indicação na fatura do n.º de requisição:

100% a 86%	Conforme ou pontuais não conformidades na indicação na fatura do número da requisição
85% a 71%	Carácter sistemático de não conformidades relativamente à indicação na fatura do número da requisição
70% a 0%	Não conforme (ausência de menção na fatura do número da requisição)

- iv. *Flexibilidade (F)* – capacidade de resposta na resolução de problemas imprevistos (assistência técnica) e/ou solicitações urgentes:

100% a 86%	Boa capacidade de resposta a solicitações urgentes e na resolução de problemas técnicos
85% a 71%	Razoável capacidade de resposta a solicitações urgentes e na resolução de problemas técnicos
70% a 0%	Limitada capacidade de resposta ou não responde

- v. *Disponibilidade de Contacto (Dc)* – avalia a disponibilidade do fornecedor para ser contactado e/ou responder em tempo oportuno a solicitações:

100% a 86%	Sempre disponível ou com retorno atempado
85% a 71%	Razoável disponibilidade ou com retorno dilatado
70% a 0%	Dificuldade de contacto

- vi. *Capacidade de Resolução de Problemas (Crp)* – avalia a capacidade para resolução de problemas/soluções alternativas:

100% a 86%	Boa capacidade de resolução de problemas ou <u>ocorrências pontuais</u> na resolução <u>sem</u> consequências significativas no desempenho
85% a 71%	Razoável capacidade de resolução de problemas
70% a 0%	Deficiente capacidade de resolução de problemas

- vii.** *Assinatura do Código Conduta fornecedores (CC) – avalia o compromisso definido no Código de Conduta de Fornecedores da Porto Ambiente;*

100%	Assinatura do Código de Conduta de Fornecedores da Porto Ambiente
5%	Não assinatura do Código de Conduta de Fornecedores da Porto Ambiente

- viii.** *Promoção de Requisitos Sustentáveis - procurement sustentável (REQ SUST) – avalia o cumprimento dos requisitos sustentáveis;*

100%	Apresenta de uma forma clara e inequívoca evidência que demonstre os requisitos sustentáveis
5%	Não apresenta de forma clara e inequívoca evidência que demonstre os requisitos sustentáveis

4. Com base na pontuação atribuída a estes critérios, será calculado, para cada fornecedor, o respetivo Índice de Qualidade do Fornecedor (IQF), utilizando para o efeito a seguinte expressão:

$$IQF = 0,6X(0,6q+0,3p+0,1admt) + 0,4x(0,4F+0,1D+0,3Crp+ 0,1CC+0,1REQ SUST)$$

Aprovado	[100 a 86]	Fornecedor de elevada confiança - risco de falha diminuto com base num histórico de desempenho isento ou quase isento de falhas.
----------	------------	--

Sugestões de Melhoria	[85 a 71]	Fornecedor de confiança - risco de falha baixo com base num histórico de desempenho regular.
Reprovado	< 70	Fornecedor de risco – risco de falha é elevado com base num histórico de desempenho irregular que não oferece confiança no cumprimento das obrigações.

Cláusula 10.ª

Código de Conduta para Fornecedores e Subcontratados da Porto Ambiente

1. O Código de Conduta para Fornecedores e Subcontratados da Porto Ambiente visa contribuir positivamente para o desenvolvimento económico, social e ambiental, na relação de compromisso, e de boa-fé, com os seus Fornecedores e Subcontratados no desenvolvimento da sua atividade, com base nos princípios consagrados na Declaração Universal dos Direitos Humanos, nas Convenções da Organização Internacional do Trabalho e na legislação nacional e europeia em vigor, constando do **Anexo VI** ao Convite à apresentação de proposta.
2. Com a apresentação dos documentos de habilitação, o Contraente Privado deve entregar a Declaração de Compromisso referida na alínea f) do n.º 1 do artigo 21.º do Convite à apresentação de proposta.

Cláusula 11.ª

Requisitos Sustentáveis

O Contraente Privado, tendo em vista garantir o desenvolvimento sustentável da sua atividade em prol da proteção do meio ambiente e dos princípios e direitos fundamentais dos trabalhadores, assumirá a responsabilidade de:

- a) disponibilizar nas suas instalações recipientes para a recolha diferenciada

de papel, embalagens, vidro e resíduos indiferenciados e proceder à remoção e à deposição dos mesmos (reciclagem ou eliminação) de acordo com as Boas Práticas da Gestão Ambiental e com as normas nacionais e internacionais de tutela do ambiente;

- b) assegurar que os materiais utilizados na execução do contrato foram fabricados em pleno respeito pelos princípios éticos e de proteção do trabalhador, nomeadamente pelas normas aprovadas pela Organização Internacional do Trabalho.

Cláusula 12.ª

Obrigações e deveres do Contraente Privado

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 Contraente Privado as seguintes obrigações principais:

- a) a execução dos serviços de acordo com as especificações descritas no Capítulo II – Cláusulas Técnicas do presente Caderno de Encargos;
- b) A manutenção da validade de todas as autorizações legalmente exigidas para o exercício das atividades inerentes à prestação de serviços;
- c) o pagamento de quaisquer encargos relativos à execução do Contrato e que, nos termos do presente Caderno de Encargos, não sejam da responsabilidade da Porto Ambiente;
- d) garantir a adoção e o cumprimento das medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação utilizadas pela Porto Ambiente, tendo em conta os princípios e regras gerais previstos no artigo 3.º do Decreto-Lei n.º 65/2021, de 30 de julho, e as normas constantes dos artigos 9.º e 10.º do mesmo diploma legal;
- e) garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes;

f) tomar as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade dos seus serviços;

g) proceder às notificações de incidentes, nomeadamente, ao Centro Nacional de Cibersegurança, de acordo com o previsto no Capítulo IV do Decreto-Lei n.º 65/2021, de 30 de julho e no regime jurídico da segurança do ciberespaço;

h) garantir o cumprimento pela Porto Ambiente das obrigações decorrentes da aplicação do Decreto-Lei n.º 65/2021, de 30 de julho, designadamente:

- i) gerir, controlar, monitorizar e apoiar na mitigação/bloqueio e reporte de incidentes de segurança informáticos, no sentido de dotar a Porto Ambiente de capacidade de resposta face aos mesmos, através da deteção, mitigação/bloqueio e resposta a ameaças conhecidas e "zero-day";
- ii) fornecer, através da capacidade de resposta referida na subalínea anterior, recursos de segurança essenciais para maximizar a visibilidade de segurança e a gestão de conformidade, incluindo descoberta de ativos, avaliação e análise de vulnerabilidades, correlação de logs/eventos (SIEM), resposta a incidentes, análise de risco, gestão de logs, relatórios de compliance (SOX, ISO27001, RGPD,...), alertas por email, ticketing integrado / alertas, monitorização comportamental, análise forense, monitorização da darkweb e MSS (Managed Security Services);
- iii) manter estes recursos atualizados contra as últimas vulnerabilidades, com atualização contínua e permanente de inteligência face a novas ameaças, num formato 24x7.

2. Para efeitos do disposto no n.º 1, entende-se por "incidente" o evento com um efeito adverso real na segurança das redes e dos sistemas de informação.

3. A título acessório, o Contraente Privado 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.

4. O Contraente Privado deve também garantir condições de segurança e saúde do trabalho a todos os seus colaboradores, cumprindo a legislação aplicável nesta matéria, nomeadamente evidenciando a identificação de perigos e a avaliação de riscos dos trabalhadores que exercem funções na prestação de serviços e dispondo das respetivas apólices de seguros de acidentes de trabalho.

Cláusula 13.ª

Obrigações principais da Porto Ambiente

A Porto Ambiente assegurará o cumprimento das seguintes obrigações:

- a) garantir o apoio, ao longo do período de vigência do contrato, do Contraente Privado na prestação dos serviços, através da disponibilização, a seu pedido, de elementos que evidenciem a organização, os processos/procedimentos e os seus sistemas de informação de um ponto de vista técnico e funcional;
- b) fornecer documentação atualizada sobre os sistemas de informação (incluindo manuais de utilizador, relatórios de auditorias realizadas, etc.), incluindo sobre os processos, procedimentos e políticas alvo de análise e disponibilizar elementos capacitados e autorizados a responder a questionários de levantamento de informação que lhe sejam dirigidos pelo Contraente Privado;
- c) assegurar os recursos (conetividade, HW e SW com o adequado licenciamento) para a preparação e instalação da(s) máquina(s) virtual(ais) que constitui(em) o(s) SIEM/MSS;
- d) Disponibilizar a necessária capacidade de armazenamento, computação e licenciamento para o volume que pretenda armazenar, caso, por questões de conformidade ou outras, a Porto Ambiente pretenda arquivar logs para retenção por período superior a 90 dias;

e) garantir que estejam ativos os contratos de manutenção das tecnologias licenciadas e a licenciar, que contribuam com informação para o serviço de SOC do Contraente Privado;

f) garantir todas as condições logísticas, de forma que a equipa do Contraente Privado possa desenvolver os trabalhos propostos (ex. espaço razoável para acomodar a equipa de Projeto caso exista necessidade de execução de trabalhos nas instalações da entidade adjudicante).

Cláusula 14.ª

Acompanhamento da execução do contrato

1. Para o acompanhamento da execução do contrato, deverá o Contraente Privado, sempre que necessário, reunir com os representantes da Porto Ambiente.
2. As reuniões previstas no número anterior devem ser alvo de uma convocatória escrita por parte do Contraente Privado, o qual deve elaborar a agenda prévia contendo os assuntos a debater.
3. O Contraente Privado deve indicar um interlocutor único para apoio/esclarecimento de dúvidas, incluindo no respeitante ao estado de execução do contrato, o qual, sempre que para o efeito solicitado, deverá deslocar-se às instalações da Porto Ambiente.

Cláusula 15.ª

Gestor do Contrato

Com vista ao acompanhamento permanente da execução do *Contrato* e nos termos do disposto no artigo 290.º-A do Código dos Contratos Públicos, é designado como *Gestor do Contrato* o Dr. Paulo Cruz, Diretor Financeiro e dos Sistemas e Tecnologias de Informação da *Porto Ambiente*.

Cláusula 16.ª

Alterações ao contrato

1. Qualquer intenção de modificação do Contrato deverá ser comunicada pela parte interessada à outra parte.

2. Qualquer modificação ao Contrato terá que ser efetuada por escrito e assinada pelos sujeitos legais ou estatutariamente habilitados para representar o Contraente Público e o Contraente Privado.
3. Qualquer modificação ao Contrato terá de observar os fundamentos e os limites previstos nos artigos 311-312.º e 313.º do CCP, respetivamente.
4. No decurso da execução do contrato, o Contraente Privado, por sua iniciativa, não poderá efetuar qualquer alteração às condições contratualmente acordadas.

Cláusula 17.ª

Cessão da posição contratual e Subcontratação

1. A cessão, total ou parcial, da posição contratual do Contraente Privado e a subcontratação, sob qualquer forma, de outra entidade terceira para execução do contrato, dependem de autorização escrita da Porto Ambiente.
2. Para efeitos do disposto no número anterior, o pedido de autorização deve ser formulado com pelo menos 30 dias de antecedência relativamente à data prevista para a outorga do acordo de cessão ou de subcontratação.
3. O pedido de autorização previsto no número anterior deve ser instruído com a minuta de acordo de cessão ou de subcontratação.

Cláusula 18.ª

Patentes, Licenças e marcas registadas

1. São da responsabilidade do Contraente Privado quaisquer encargos decorrentes da utilização de marcas registadas, patentes, licenças ou outros títulos no âmbito da propriedade intelectual ou industrial.
2. Caso a Porto Ambiente venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o Contraente Privado indemniza-a de todas as despesas que, em

consequência, tenha de assumir e de todas as quantias que tenha de pagar, seja a que título for.

Cláusula 19.ª

Confidencialidade e Proteção de dados pessoais

1. O Contraente Privado não está autorizado, durante a vigência do Contrato e após a sua cessação, a divulgar e reproduzir, parcial ou totalmente, todas e quaisquer informações ou documentação, técnica e não técnica, comercial ou outra, que lhe tenha sido confiada pela Porto Ambiente ou que tenha tido conhecimento no âmbito do Contrato.
2. Os dados pessoais a que o Contraente Privado tenha acesso ou que lhe tenham sido transmitidos pela Porto Ambiente ao abrigo do Contrato, serão tratados em estrita observância das regras e normas nacionais e europeias observadas pelo Contraente Público.
3. O Contraente Privado 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 Porto Ambiente ao abrigo do Contrato, sem que para tal tenha sido expressamente autorizado pela mesma por escrito.
4. No caso em que o Contraente Privado seja autorizado pela Porto Ambiente a subcontratar outras entidades para a realização da sua prestação contratual, nos termos da Cláusula 18.ª, o mesmo será o único responsável pela escolha das empresas subcontratadas bem como por toda a atuação destas, incluindo designadamente pelo cumprimento do disposto na presente cláusula.
5. O Contraente Privado compromete-se, na qualidade de subcontratante, a dar pleno e integral cumprimento às obrigações decorrentes da legislação europeia e nacional de proteção de dados pessoais, devendo registar e reportar periodicamente à Porto Ambiente, no máximo trimestralmente, as atividades desenvolvidas neste âmbito e as medidas técnicas e

organizativas implementadas que se mostrem adequadas à proteção da confidencialidade e segurança dos dados objeto de tratamento, incluindo, quando seja caso disso, a realização da competente avaliação de riscos, devendo tais obrigações constar dos contratos escritos que o Contraente Privado celebre com outras entidades por si subcontratadas.

6. O Contraente Privado obriga-se, em matéria de tratamento de dados pessoais, nomeadamente a:
 - a) utilizar os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pela Porto Ambiente única e exclusivamente para efeitos da realização das prestações compreendidas no objeto do Contrato, procedendo à recolha, ao tratamento, à consulta, à conservação e ao registo dos dados pessoais que se afigurem estritamente necessários e em conformidade com as finalidades exclusivas subjacentes ao Contrato, assim como à eliminação dos mesmos dados após o termo do Contrato;
 - b) manter os dados pessoais estritamente confidenciais, cumprindo e garantindo o cumprimento do dever de sigilo profissional relativamente aos mesmos dados pessoais;
 - c) pôr em prática as medidas técnicas e de organização necessárias à proteção dos dados pessoais tratados por conta da Porto Ambiente contra a respetiva destruição, accidental ou ilícita, a perda accidental, a alteração, a difusão ou o acesso não autorizado, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais;
 - d) proceder aos tratamentos previstos no número anterior apenas por profissionais sujeitos a sigilo profissional e a dever de confidencialidade, devendo ser-lhes ministrada formação específica na área da proteção de dados pessoais;
 - e) prestar à Porto Ambiente toda a colaboração de que esta careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais efetuados ao abrigo do Contrato e manter a Porto Ambiente

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;

- f) assegurar que os seus Colaboradores cumprem todas as obrigações previstas no Contrato, incluindo designadamente em matéria de proteção de dados pessoais;
 - g) designar um representante ou, quando aplicável, indicar o encarregado de proteção de dados que será o responsável junto da Porto Ambiente nas matérias a que se refere a presente cláusula.
7. O Contraente Privado será responsável por qualquer prejuízo em que a Porto Ambiente venha a incorrer em consequência do tratamento, por parte da mesma e/ou dos seus colaboradores, de dados pessoais em violação das normas legais aplicáveis e/ou do disposto no Contrato.
8. Para efeitos do disposto nos números anteriores, entende-se por “colaborador” toda e qualquer pessoa singular ou coletiva que preste serviço ao Contraente Privado, incluindo, designadamente, representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido entre o Contraente Privado e o referido colaborador.

Cláusula 20.ª

Sigilo

1. O Contraente Privado deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à Porto Ambiente, de que possa ter conhecimento ao abrigo ou em relação à 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, tanto durante a sua vigência como após a sua cessação.

3. Excluem-se do dever de sigilo previsto nesta cláusula a informação e a documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo Contraente Privado ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido das entidades reguladoras ou de outras entidades administrativas competentes.

Cláusula 21.ª

Causas de Força Maior

1. Não podem ser impostas penalidades ao Contraente Privado, nem é tida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de causa de força maior ou que não lhe seja imputável, entendendo-se como tais 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 consubstanciar uma causa de força maior, nos termos do número anterior, nomeadamente 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 constituem força maior para os subcontratados do Contraente Privado, na parte em que intervenham;

- b) Greves ou conflitos laborais limitados às sociedades do Contraente Privado ou a grupos de sociedades em que este se integre, bem como a sociedade ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo Contraente Privado de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo Contraente Privado de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do Contraente Privado, 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 Contraente Privado não devidas a sabotagem e pelos quais o mesmo não deva ser responsabilizado;
 - g) Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar causas 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 22.ª

Sanções contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, das especificações e do planeamento, a Porto Ambiente pode exigir ao Contraente Privado o pagamento de uma quantia pecuniária, de

montante a fixar em função da gravidade do incumprimento, da culpa, da situação económica e do benefício económico que aquele tiver retirado do incumprimento, nos seguintes termos:

- a) Por cada mês que o Contraente Privado, por sua responsabilidade, não cumpra as obrigações constantes da cláusula 13.ª, ou as atividades objeto da prestação de serviços previstas no Capítulo II – Cláusulas técnicas deste caderno de encargos, será aplicada uma sanção calculada de acordo com a seguinte fórmula:

$$\text{VS: [NMF*(25\%*VMVT)]}$$

Em que:

VS: Valor da sanção

NMF: N.º meses de não cumprimento

VMVT: Valor mensal contratualizado

2. Em caso de resolução do contrato por incumprimento do Contraente Privado, a Porto Ambiente pode exigir-lhe uma pena pecuniária de montante correspondente ao dobro do valor da penalidade estabelecida no número anterior.
3. Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo Contraente Privado ao abrigo da alínea a) do n.º 1, relativamente aos serviços cujo atraso na respetiva conclusão tenha determinado a respetiva resolução do contrato.
4. Na determinação da gravidade do incumprimento, a Porto Ambiente tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do Contraente Privado e as consequências do incumprimento.
5. A Porto Ambiente 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 Porto Ambiente exija uma indemnização pelos danos decorrentes da mora no cumprimento, cumprimento defeituoso e incumprimento definitivo, nos termos gerais da responsabilidade civil.
7. Sem prejuízo do disposto na cláusula seguinte, o valor acumulado das sanções contratuais a aplicar não poderá exceder o montante correspondente a 20% do preço contratual.

Cláusula 23.ª

Resolução do contrato pela Porto Ambiente

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a Porto Ambiente pode resolver o contrato no caso de o Contraente Privado violar, de forma grave, qualquer das obrigações que lhe incumbem.
2. O direito de resolução referido no número anterior exerce-se mediante declaração expressa enviada ao Contraente Privado.

Cláusula 24.ª

Comunicações e notificações

1. Todas as notificações e comunicações relativas à fase de formação de contrato devem ser escritas e redigidas em português e efetuadas através de correio eletrónico ou de outro meio de transmissão escrita e eletrónica de dados.
2. As comunicações relativas à fase de execução do contrato podem ser efetuadas pelos meios a que se refere o número anterior, ou por via postal, por meio de carta registada com aviso de receção.
3. Qualquer alteração das informações de contacto das partes deve ser comunicada à outra parte e ser reduzida a escrito, sem o que não produz qualquer efeito.

4. Para incidentes de segurança que tenham sido verificados internamente pela Porto Ambiente, deve esta utilizar um dos seguintes meios (conforme a prioridade):
- i. Plataforma de Ticketing / Workflow que será disponibilizada pelo h-SOC do Contraente Privado;
 - ii. Email: soc@hardsecure.com;
 - iii. Telefone, após o qual terá que ser utilizado um meio escrito previsto nas alíneas anteriores.

Cláusula 25.ª

Contagem dos prazos

Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados, nos termos do artigo 471.º do CCP.

Cláusula 26.ª

Foro competente

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

Cláusula 27.ª

Legislação aplicável

Em tudo o que estiver omissa no presente Caderno de Encargos será observado o disposto no Código dos Contratos Públicos e na demais legislação portuguesa aplicável.

CAPÍTULO II

CLÁUSULAS TÉCNICAS

Cláusula 28.ª

Âmbito de aplicação

A presente prestação de serviços visa assegurar a conformidade da atividade desenvolvida pela Porto Ambiente com os requisitos e normas previstas no Decreto-Lei n.º 65/2021, de 30 de julho, nomeadamente:

a) Os requisitos de segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública e pelos operadores de serviços essenciais, nos termos dos artigos 12.º, 14.º e 16.º do Regime Jurídico da Segurança do Ciberespaço;

b) Os requisitos de notificação de incidentes que afetem a segurança das redes e dos sistemas de informação, prevendo as circunstâncias, o prazo, o formato e os procedimentos aplicáveis, nos termos dos artigos 13.º, 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço e do Capítulo IV do Decreto-Lei n.º 65/2021, de 30 de julho

Cláusula 29.ª

Atividades para avaliação do Sistema de Gestão de Segurança da Informação

A prestação de serviços deverá contemplar, nomeadamente, o seguinte universo de atividades para avaliação do Sistema de Gestão de Segurança da Informação (SGSI):

a) Levantamento de situações anómalas (algumas delas poderão ser repetidas);

b) Levantamento de políticas, processos e procedimentos de segurança e de resposta a incidentes de segurança;

c) Recolha da informação de registo (*logs*), providenciando a monitorização aos principais portais, para avaliação de riscos e vulnerabilidades (verificação do estado atual da estrutura de IT);

- d) Recolha e monitorização de informação da estrutura IT da Porto Ambiente, bem como questões realizadas a indivíduos com diferentes graus de responsabilidade na sua estrutura funcional, a ser executado com base no *Checklist Information Security Management BS ISO/IEC 27001:2013*;
- e) Recolha das configurações de *switching* e *routing* (layer 2 e 3) para análise das metodologias de segurança utilizadas pela Porto Ambiente ao nível de *networking*;
- f) Recolha de informação sobre a arquitetura e tecnologias utilizadas em toda a estrutura IT, com principal ênfase na DMZ;
- g) Identificação e análise dos ativos de rede, nos termos e em conformidade com o previsto no artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho;
- h) Identificação dos servidores (independentemente do sistema operativo) para verificação de GPOs, portas/protocolos e serviços disponibilizados.

Cláusula 30.ª

Atividades Técnicas

1. A prestação de serviços deverá contemplar, nomeadamente, as seguintes atividades técnicas:

a) Políticas de Segurança da Informação:

i. gestão e atualização das políticas de segurança da informação da Porto Ambiente;

b) Organização da Segurança da Informação:

i. gestão da informação da Porto Ambiente incluindo: identificação de regras e responsabilidades, segregação de funções, dispositivos móveis e *teleworking*;

c) Segurança dos Recursos Humanos:

i. gestão dos recursos humanos da Porto Ambiente, durante e após a contratação;

d) Gestão de Ativos:

i. gestão dos ativos da Porto Ambiente;

e) Controlo de Acessos:

i. gestão e controlo de acessos à informação da Porto Ambiente;

f) Criptografia:

i. controlo do uso da criptografia dentro da Porto Ambiente;

g) Segurança Física e ambiental:

i. gestão e controlo da organização física e acesso ambiental;

h) segurança das operações:

i. gestão e controlo de todas as operações, incluindo procedimentos operacionais e responsabilidades, *logging* e monitorização, gestão de vulnerabilidades técnicas e auditoria aos sistemas de informação;

i) segurança das comunicações:

i. gestão e controlo da segurança das comunicações da Porto Ambiente, incluindo gestão da segurança da rede e controlos na transferência de informação;

j) aquisição de sistemas, desenvolvimento e manutenção:

i. gestão e controlo do ciclo de desenvolvimento de sistemas, incluindo: identificação, controlo de qualidade de código, segurança dos sistemas em desenvolvimento;

k) Relação com fornecedores:

i. Gestão da relação com fornecedores, incluindo aplicação da segurança da informação na relação com fornecedores e gestão na entrega de serviços à Porto Ambiente;

l) Gestão de incidentes de segurança da informação:

i. Gestão, controlo e monitorização de incidentes de segurança da informação;

m) Aspetos da segurança da informação na continuidade de negócio:

i. Gestão da continuidade da segurança da informação e redundâncias;

n) *Compliance*:

i. Gestão da *compliance* da Porto Ambiente com requisitos legais e contratuais.

2. Os controlos de área que poderão ser aplicáveis à Porto Ambiente com base na norma ISO 27001:2013 e ISO27005 serão definidos de acordo com o modelo de negócio da instituição.

Cláusula 31.ª

Análises Técnicas

Na sequência da prática das atividades técnicas, serão originadas as seguintes análises:

a) Ao nível aplicacional da Porto Ambiente, onde serão analisados o uso de tecnologias menos recentes em praticamente todas as áreas de atuação e as políticas de autenticação definidas internamente para determinados processos, sendo efetuada a análise a aplicações WEB que estejam expostas a ataques realizados internamente e externamente;

b) Das propriedades ACID (Atomicidade, Consistência, Isolamento e Durabilidade) e testes de *benchmark* TPC-C de forma a avaliar o modelo de dados (*sql schema*);

- c) Dos sistemas ativos de segurança, indicando quais as assinaturas ativas para cada funcionalidade;
- d) Da informação que será possível recolher, sendo analisadas as várias DMZ em termos de arquitetura e infraestruturas periféricas e respetiva performance, ao nível de pedidos executados internamente;
- e) Das políticas e normas de segurança da informação existentes na Porto Ambiente, incluindo a verificação de conformidades, como por exemplo, páginas de negação WEB, *banners*, políticas de segurança decididas ao mais alto nível e difundidas por toda a estrutura da entidade;
- f) Da forma como são realizadas as atualizações de portais e outros sistemas, bem como a sua manutenção, no sentido de verificar a existência de ficheiros com informação sobre instalação de atualizações e que possam fornecer demasiada informação interna;
- g) Das regras e políticas configuradas nos sistemas ativos de segurança;
- h) Da capacidade em detetar e prevenir ataques, através de equipas de monitorização contra intrusões;
- i) Das permissões de acesso à rede, verificando se existe algum controlo sobre os colaboradores da Porto Ambiente para instalação de *software*;
- j) Da existência de protocolos de autenticação segura, bem como de colocação das máquinas em quarentena caso não cumpram os requisitos de segurança estabelecidos pela Porto Ambiente;
- k) As vulnerabilidades existentes nas aplicações e Bases de Dados (com respetivos conectores), independentemente do nível/grau de programação/linguagem utilizada, *frameworks* sobre as quais estão assentes e respetivos sistemas operativos.

Cláusula 32.ª

Descrição das Atividades Técnicas para resposta a incidentes de segurança

Com vista a dar resposta a incidentes de segurança, o Contraente Privado deverá adotar as seguintes atividades técnicas:

a) Implementação de Contramedidas:

Estas medidas serão adotadas em coordenação com a equipa técnica do Contraente Privado, sendo um trabalho executado de forma muito próxima com a equipa de operações de rede/TI da Porto Ambiente (ou de entidade terceira que dê suporte e manutenção à empresa);

A análise de segurança imediata e das funções de gestão de configurações dos ativos de segurança será orientada pelo gestor de projeto para coordenação das atividades, a ser designado pelo Contraente Privado nos termos do n.º 3 da cláusula 15.ª;

b) Monitorização em Tempo Real e Análise da Triagem / Incidente:

Deverá ser executada a observação dos dados não tratados, bem como a primeira análise à informação dos dados veiculados pelos utilizadores finais.

O Contraente Privado poderá provavelmente ter recebido relatórios de incidentes de outros SOC's de entidades similares com o reporte do mesmo incidente;

c) Análise de Vulnerabilidades e *Penetration Testing*:

O Contraente Privado deverá executar e coordenar estas atividades, bem como um conjunto de ações de *ethical hacking* e abordagens proativas (XSS, RFI/LFI, *Defacing*, *Land Attack*, *Fuzzing*, *SQLi*, entre outros) e bem assim as atividades de *Assessment Vulnerability / Penetration Testing* (VA/PT);

O Contraente Privado deverá proporcionar uma base única para visualizar o ambiente da Porto Ambiente e aumentar a visibilidade do risco de segurança para qual a entidade está exposta;

O Contraente Privado deverá avaliar o estado de segurança de serviços publicados na intranet/internet (independentemente do serviço, aplicação, porta ou protocolo disponibilizado pela Porto Ambiente) e integrado com o MSS para dar uma completa visibilidade e perceção do que é possível fazer dentro e fora da empresa, sendo executados um conjunto de controlos e técnicas ao nível de *Ethical/White hacking*, no sentido de garantir que ataques realizados por *hackers* com intenções maliciosas sejam minimizados.

A Porto Ambiente deverá ser apoiada nas respetivas correções/mitigações a realizar sempre que sejam identificadas vulnerabilidades (categorização CVE - *Common Vulnerabilities and Exposures*) e categorizadas de acordo com o standard ISO 27005 e conforme o *Common Vulnerability Scoring System (CVSS)*, de acordo com os SLA's acordados com a empresa em sede de execução do contrato.

cc) Gestão de vulnerabilidades e testes de intrusão

Relativamente à gestão de vulnerabilidades e testes de intrusão, o Contraente Privado deverá efetuar uma análise aos sistemas e aplicações da Porto Ambiente (*Grey Box* e *White Box*), incidindo sobre todos os IP's com serviços ativos publicados pela empresa no âmbito definido para este contrato, em função das vulnerabilidades que possam vir a ser identificadas e/ou em resposta a solicitações por parte da Porto Ambiente.

As ferramentas a utilizar serão selecionadas de acordo com os resultados das fases de recolha de informação e de acordo com o conhecimento que se irá gerar com o decorrer dos testes.

Desta forma, para levantamento de vulnerabilidades, análise do risco e execução de testes de intrusão com injeção de incidentes informáticos (esta

fase será executada em coordenação com a equipa de IT da Porto Ambiente ou de entidades terceiras que prestam serviço a esta instituição), será necessária a realização de um conjunto de fases exploratórias.

A equipa do contraente privado deverá seguir as metodologias standard indicadas para a conjugação dos controlos A.12, A.13 e A.14 do standard ISO27001:2013, normalmente dividido nas seguintes secções:

- Pre-engagement Interactions
- Intelligence Gathering
- Exploitation
- Post Exploitation
- Reporting
- Threat Modeling
- Vulnerability Analysis

d) Mapeamento de Rede / *Vulnerability Scanning*:

Estas atividades podem ser vistas como sustentação das funções de TI em vez de funções de operações de segurança. Os mapas de rede atualizados e as estatísticas de vulnerabilidades, são registos determinantes para o esforço na análise de incidentes;

e) Ferramentas de Engenharia:

Dado que a Porto Ambiente gere consolas de soluções de segurança internamente / depende de uma entidade externa (suporte e manutenção de Firewalls, IDS/IPS, Antivírus, CMS, DLPs,...), esta atividade terá de ser coordenada com o gestor de projeto designado pelo Contraente Privado;

f) Tuning dos Sensores:

O Contraente Privado deverá utilizar os seus próprios sensores de monitorização via SIEM, *Honeypots*, *Vulnerability Assessments*, IDS, etc. Esta

atividade deverá ser considerada um requisito para qualquer opção que implementa a capacidade de monitorização, devendo ser um processo contínuo necessário para o correto funcionamento na obtenção de dados da Porto Ambiente, de forma a analisar a empresa do ponto de vista heurístico e comportamental, sendo, por conseguinte, uma função de operação e não uma função de engenharia ou desenvolvimento;

g) Recolher, reter e armazenar dados da Auditoria/ Criação e Gestão de Conteúdos de Auditoria:

Esta atividade é importante como benefício colateral da recolha e análise compreensiva dos *log's*.

Cláusula 33.ª

Descrição das Atividades Processuais

O Contraente Privado deverá promover, entre outras, as seguintes ações:

- IDENTIFICAÇÃO DO PONTO DE CONTACTO PERMANENTE E DO RESPONSÁVEL DE SEGURANÇA: Deverão ser nomeados pelo Conselho de Administração da Porto Ambiente:

- i. Um elemento da Porto Ambiente como Responsável de Segurança;
- ii. o(os) elemento(os) e respetivo(os) contacto(os) da organização, como Ponto de Contacto Permanente (elemento do Contraente Privado ou da Porto Ambiente, a definir posteriormente);
- iii. um elemento da Porto Ambiente, como ponto de contacto com o Contraente Privado (de acordo com a Cláusula 15.ª do Caderno de Encargos), por forma a serem estabelecidos os canais de comunicação necessários e os procedimentos de notificação;

Ao Ponto de Contacto Permanente referido na alínea ii, do ponto de vista técnico/operacional, incumbirá responder às solicitações da equipa operacional do CNCS (CERT.PT), sendo inclusive esperada disponibilidade para contactos de emergência, fora do horário de expediente.

- IDENTIFICAÇÃO DE FUNÇÕES OU ATIVIDADES CRÍTICAS: o Contraente Privado deverá identificar os processos de negócio na Porto Ambiente, por forma a identificar as prioridades nos respetivos processos e a criticidade inerente aos seus serviços. Esta informação importante, associada à dos endereços IP públicos associados, permitirá ao Contraente Privado, a partir de eventos de cibersegurança recolhidos de outras fontes, identificar rapidamente possíveis ameaças ou ataques em curso que envolvam a organização e/ou a função ou atividade associada. Deverão ser definidos os processos mais importantes para a Porto Ambiente, por forma a ordená-los por criticidade, identificando potenciais ameaças e consequentes impactos, identificando ainda dependências internas e externas entre sistemas, permitindo assim construir o denominado quadro global de ameaças da Porto Ambiente.
- ESTABELECIMENTO DE CANAIS DE COMUNICAÇÃO: No que concerne à troca de informação por correio eletrónico, como é consabido, muita desta mesma informação (principalmente no que refere a detalhes sobre ameaças, incidentes ou vulnerabilidades) é bastante sensível. Assim sendo, esta deverá ser encriptada, sendo que todas as partes envolvidas terão as próprias chaves PGP (ou outras a definir).
- REGISTO DE ENDEREÇOS IP NO LIR (*LOCAL INTERNET REGISTRY*): A base de dados do LIR é a principal fonte de informação de contacto para a comunidade internacional de resposta a incidentes e para o CNCS em particular. A Porto Ambiente terá esta informação atualizada, uma vez que permitirá à organização receber notificações e outra informação de cibersegurança relevante para as redes e sistemas sob a sua responsabilidade.
- ANÁLISE DE RISCO: A gestão do risco é o processo contínuo de identificação, avaliação e resposta ao risco. No caso em concreto e no seguimento dos serviços críticos, deverão ser realizadas as análises de risco necessárias, por forma a:

i) Identificar as vulnerabilidades associadas a esses serviços e as ameaças a que a que se encontram expostos;

ii) Calcular a probabilidade de concretização da ameaça e o impacto daí esperado;

iii) Avaliar a criticidade de cada um dos ativos, baseada no impacto decorrente de uma eventual falha de segurança (nível de risco).

- CADEIA DE RESPONSABILIDADE: Deverá ser definida a cadeia de responsabilidade, podendo a mesma ser ajustada ao longo de todo o processo. Serão definidos os privilégios de acesso individual, tendo em conta as funções desempenhadas e as responsabilidades inerentes, sendo posteriormente dado conhecimento à Porto Ambiente. Deverá iniciar-se com a formação do Responsável de Segurança, habilitando-o a detetar os incidentes de cibersegurança dentro da organização, definindo, diligenciando e aprovando os processos de deteção de incidentes que se afigurem adequados.

- POLÍTICA DE SEGURANÇA: Deverá ser elaborada uma Política de Segurança de Informação adequada à Porto Ambiente, atendendo às suas necessidades e responsabilidades. A sua efetivação verificar-se-á mediante os processos e procedimentos específicos que serão implementados por cada departamento da organização.

- PROCEDIMENTOS DE NOTIFICAÇÃO DE INCIDENTES: Deverá ser elaborado um procedimento de notificação de incidentes de cibersegurança, com impacto nas funções ou atividades identificadas como críticas.

- RELATÓRIO ANUAL DE SEGURANÇA: Deverá ser elaborado um relatório anual que observe os requisitos definidos no artigo 8.º do Decreto-Lei n.º 65/2021, de 30 de julho.

Cláusula 34.ª

Descrição das Atividades de Desenvolvimento da arquitetura de segurança

Nesta fase deverão ser promovidas ações com vista a dotar a organização dos principais recursos processuais e técnicos de base para uma defesa eficaz dos seus ativos, quer a nível de perímetro de rede, quer de servidores, postos de trabalho e outros dispositivos. Deverão ser executadas, entre outras, as seguintes ações:

- **DESENHO E IMPLEMENTAÇÃO DA ARQUITETURA E SEGURANÇA PERIMÉTRICA:** Aplicando os princípios de uma abordagem por camadas de segurança com base na análise de risco realizada, deverá conceber-se uma nova arquitetura de cibersegurança para a organização (caso se aplique), por forma a organizar as várias áreas de segurança, identificando as necessidades de deteção de eventos anómalos com origem no exterior e entre zonas de segurança distintas.
- **IMPLEMENTAÇÃO DE UM SISTEMA DE RECOLHA E ARMAZENAMENTO DO FLUXO DE TRÁFEGO:** Deverá ser implementado um sistema de recolha do fluxo de tráfego, de acordo com os recursos tecnológicos adquiridos/fornecidos pela organização. Note-se que este é um instrumento essencial para identificar padrões de comunicação com sistemas potencialmente comprometidos e analisar tráfego considerado malicioso.
- **COMUNICAÇÃO COM O CNCS:** Deverá ser definido um procedimento de comunicação entre a Porto Ambiente e o CNCS que permita à empresa dar cumprimento a todas as obrigações respetivas consubstanciadas no Decreto-Lei n.º 65/2021, de 30 de julho.
- **INVENTARIAÇÃO DE ATIVOS / PRODUÇÃO DE UM MAPA DE REDES:** Deverá ser elaborado e permanentemente atualizado um inventário de ativos, nos termos e em conformidade com o exigido pelo artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho, devendo igualmente ser analisado o diagrama existente com

as principais infraestruturas de comunicações de dados e os sistemas de suporte aos serviços críticos da organização.

- **VERIFICAÇÃO DA RECOLHA CENTRALIZADA DE REGISTOS (LOGS):** Uma vez que os logs produzidos pelo sistema operativo e pelas aplicações de suporte à atividade são o principal instrumento de análise e investigação de um incidente de cibersegurança, deverá ser verificado se a organização possui um repositório central para estes logs e qual o prazo de armazenamento dos mesmos.
- **CRIAÇÃO DE INSTRUMENTOS DE CORREÇÃO OU MITIGAÇÃO DE INCIDENTES:** Dependendo da origem do incidente em causa, em que será necessário aplicar medidas corretivas ou de mitigação, deverão ser criados os devidos instrumentos de correção e/ou mitigação.
- **CONFORMIDADE COM A LEGISLAÇÃO APLICÁVEL E NORMAS DA ÁREA DE ATIVIDADE:** Deverá ser realizada uma análise tendo em vista garantir a conformidade da atuação da Porto Ambiente com as normas legais e regulamentares aplicáveis, incluindo em especial o Decreto-Lei n.º 65/2021, de 30 de julho.
- **CRIAÇÃO DE UMA POLÍTICA DE USO ACEITÁVEL(PUA):** Deverá ser elaborada uma PUA, onde estarão consignadas as linhas de orientação para a boa utilização dos recursos TIC internos.
- **MANUTENÇÃO DE INFRAESTRUTURAS DE CÓPIAS DE SEGURANÇA E REPOSIÇÃO(BACKUP/RESTORE):** Deverão ser criados mecanismos proporcionais ao risco existente de eliminação ou corrupção de dados em sistemas que são importantes para o bom funcionamento da organização.
- **AÇÕES DE FORMAÇÃO:** As ações de formação ocorrerão por forma a consolidar as ações anteriores. Deverão ser realizadas 2 (duas) ações de formação, por ano, em formato webinar, (uma ação de formação por semestre) para todos os colaboradores da Porto Ambiente.

Cláusula 35.ª

Descrição das Atividades de Implementação

Nesta fase, deverão ser contempladas auditorias de segurança e mecanismos de supervisão, bem como a consolidação de informação de registo e monitorização no sistema integrado de gestão de eventos (SIEM):

- **DEFINIÇÃO DE PROCEDIMENTOS DE OPERAÇÃO:** Deverão ser identificados os procedimentos para a deteção de incidentes, atualização de ativos, triagem, análise de observáveis, fluxo de informação interno e de interação com entidades externas. Deverão ainda ser identificadas as responsabilidades e funções para os procedimentos acima descritos, bem como toda a sua tramitação, consoante a ocorrência em causa, sendo considerados assim diferentes cenários de atuação.
- **PLANO DE SEGURANÇA:** Deverá ser elaborado um plano de segurança, o qual conterá, nos termos do artigo 7.º do Decreto-Lei n.º 65/2021, de 30 de julho, a política de segurança, descrição das medidas organizativas, formação, identificação do responsável de segurança, bem como a identificação do ponto de contacto permanente para com o CNCS.
- **AUDITORIA DE SEGURANÇA A BASES DE DADOS:** Deverão ser realizadas auditorias de segurança às bases de dados da Porto Ambiente, por forma a atestar que a instalação e a configuração dos mecanismos das fases anteriores estão consoante as necessidades da empresa.
- **MECANISMOS DE MONITORIZAÇÃO:** o Contraente Privado deverá promover a instalação e configuração de um sistema de monitorização dos principais ativos de rede e sistemas de suporte às atividades da Porto Ambiente, o qual deverá medir indicadores de disponibilidade e de qualidade dos equipamentos e serviços, despoletando alertas sempre que o valor medido ultrapasse os parâmetros normais de funcionamento (definidos pela organização).

- *HARDENING DAS CONFIGURAÇÕES*: Deverá ser realizado um robustecimento alinhado com um mapeamento das ameaças e das ações de mitigação dos riscos, com a execução das atividades corretivas, com foco na infraestrutura.
- *SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)*: Deverá ser proporcionado o devido apoio ao sistema de gestão e correlação de dados e eventos, por forma a facilitar a análise em tempo real e a acelerar a tomada de ações defensivas, caso seja necessário.
- *SIMULACROS DE INCIDENTES DE CIBERSEGURANÇA*: Deverá ser realizado, pelo menos, um simulacro de um incidente de cibersegurança, sujeito a avaliação da Porto Ambiente.
- *DEFINIÇÃO DE PROCEDIMENTOS DE REAÇÃO A INCIDENTES*: Deverá ser promovida a identificação dos tipos de ataques mais comuns, criando-se um procedimento para a respetiva mitigação ou resolução e um procedimento interno para notificação de incidentes.
- *TESTES DE ACEITAÇÃO DE SERVIÇOS E MECANISMOS HONEYPOTS*: Deverão ser realizados os devidos e necessários testes de aceitação de serviços, submetendo as aplicações, serviços e sistemas a ataques de vários tipos e intensidades, por forma a analisar o respetivo comportamento perante esses ataques, propondo as soluções devidas. O mesmo se aplicará aos métodos de engodo (*honeypots*).
- *RESPOSTA A INCIDENTES DE SEGURANÇA*: Deverá ser promovida a Implementação de Capacidade de Resposta a Incidentes de Segurança, que poderá ser realizada pela Porto Ambiente ou pelo Contraente Privado (as a service).

Cláusula 36.ª

Descrição de Capacidades

1. Com controlos de segurança essenciais e inteligência de ameaças integrada, o h-SOC do Contraente Privado deverá permitir oferecer uma completa

Página 40 de 53

Caderno de Encargos

PRESTAÇÃO DE SERVIÇOS DE ASSESSORIA PARA CONFORMIDADE AO REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO – ADG/09/2022

visibilidade da segurança das ameaças que afetam a rede de dados da Porto Ambiente, permitindo ao mesmo tempo apoiar na sua mitigação de forma fácil e rápida, quer na Resposta a Incidentes de Segurança ocorridos internamente ou externamente (sob os serviços publicados na web) ou no alerta de incidentes que ocorreram em outros pontos externos à organização e que possam comprometer os serviços, dados ou aplicações de forma interna.

2. Deverão ser facultadas, entre outras, as seguintes capacidades de ação:

- a) Definir o âmbito e plano de governação;
- b) Conceber infraestruturas em consonância;
- c) A retenção de pacotes, fluxos de dados, Syslog e outros eventos;
- d) Recolher, correlacionar e analisar;
- e) A monitorização da informação e dos dados (verificação das vulnerabilidades que afetam todo o ecossistema da empresa);
- f) A recolha de dados eficiente e eficaz;
- g) A integração com fontes de informação & intel externas;
- h) A Resposta a incidentes de segurança – gerida através da plataforma *Unified Security Management (MSS)*;
- i) A Administração/Gestão, controlo e monitorização no hSOC;
- j) A Plataforma - > aceleração e simplificação da deteção de ameaças, respostas a incidentes de segurança, devendo o relatório relativo à Gestão de conformidades ser entregue à equipa de TI da Porto Ambiente;
- k) A Gestão de Incidentes de Segurança (*Ticketing/Workflow*), devendo ser o respetivo relatório disponibilizado em tecnologia baseada em ITIL & *Service Support*;

l) *Call Center*:

Deverá ser disponibilizado um serviço de Call Center com linha dedicada para incidentes que ocorram na empresa. O h-SOC não quer perder vestígios que, de outra forma, seriam tratados como um problema de disponibilidade. Em qualquer caso, por definição esta capacidade é garantida pelo h-SOC.

m) Implementação de Contramedidas:

Estas atividades deverão ser desenvolvidas pelo h-SOC em coordenação com a equipa técnica do Contraente Privado, sendo um trabalho executado de forma muito próxima com a equipa de operações de rede/TI da Porto Ambiente (ou de entidade terceira que dê suporte e manutenção à instituição). A análise de segurança imediata e as funções de gestão de configurações dos ativos de segurança serão atividades a desenvolver pelo gestor de projeto designado pelo Contraente Privado.

n) Monitorização em Tempo Real e Análise da Triagem / Incidente:

Esta atividade é fundamental no hSOC. Deverá ser executada a observação dos dados não tratados, bem como a primeira análise à informação dos dados veiculados pelos utilizadores finais.

o) Análise de Vulnerabilidades e *Penetration Testing*:

O h-SOC deverá possuir capacidades para executar e coordenar estas atividades, proporcionando uma base única para visualizar o ambiente da Porto Ambiente e para aumentar a visibilidade do risco de segurança ao qual a empresa esteja exposta. O h-SOC deverá executar um conjunto de ações de *ethical hacking* e abordagens proativas (XSS, RFI/LFI, *Defacing*, *Land Attack*, *Fuzzing*, *SQLi*, entre outros). Esta capacidade de *Assessment Vulnerability / Penetration Testing* (VA/PT) deverá ser integrada no MSS a instalar na Porto Ambiente.

p) Mapeamento de Rede / *Vulnerability Scanning*:

Estas atividades podem ser vistas como sustentação das funções de TI em vez de funções de operações de segurança. Os mapas de rede atualizados e as estatísticas de vulnerabilidades são registos determinantes para o esforço na análise de incidentes.

q) Ferramentas de Engenharia:

Se a Porto Ambiente gere consolas de soluções de segurança internamente ou depende de uma entidade externa (suporte e manutenção de Firewalls, IDS/IPS, Antivírus, SIEM, DLPs,...), esta atividade deverá ser desenvolvida em coordenação com o gestor de projeto do h-SOC designado pelo Contraente Privado.

r) Tunning dos Sensores:

O h-SOC deverá possuir os seus próprios sensores de monitorização que passam pelo MSS, *Honeypots*, *Vulnerability Assessments*, IDS, etc. O tuning é uma atividade interna sustentada, impulsionada pelo feedback dos analistas do h-SOC. Portanto, esta atividade deverá ser considerada um requisito para qualquer opção que implementa a capacidade de monitorização, tratando-se de um processo contínuo necessário para o correto funcionamento na obtenção de dados da Porto Ambiente de forma a promover uma análise heurística e comportamental da empresa. Será, portanto, uma função de operação e não uma função de engenharia ou desenvolvimento.

s) Recolher, Reter e Armazenar dados da Auditoria/ Criação e Gestão de Conteúdos de Auditoria:

Atividade importante como benefício colateral da recolha e análise compreensiva dos *log's*.

3. O workflow (a definição das etapas do procedimento) será definido conjuntamente entre a Porto Ambiente, parceiros e o h-SOC - gestor do projeto designado pelo Contraente Privado.

Cláusula 37.ª

Descrição de Capacidades Avançadas

O Contraente Privado deverá promover uma análise avançada de incidentes e suporte a respostas, como análise digital forense de imagens obtida a partir de memória e disco rígido, incluindo as seguintes atividades:

- Criação e afinação de análises avançadas para detetar modelos de ataque complexos ou avançados, como os utilizados para detetar e seguir os APT's através da ferramenta de MSS do h-SOC;
- Desenvolver ferramentas personalizadas orientadas para detetar, monitorizar, manter (para efeitos de investigação) ou bloquear os APT's em diferentes fases do ciclo de vida dos ciberataques;
- Exercer e completar uma capacidade de gestão do conhecimento das ameaças, permitindo que os analistas do SOC interliguem atividades, incidentes, indicadores e diferentes artefactos;
- Acompanhar tendências e elaborar relatórios de atividades e incidentes relacionados com os APT's;
- Investigação da presença de APT's em redes monitorizadas pelo h-SOC;
- *Honeypotting* e outros métodos de recolha que permitam à célula recolher, analisar, investigar e monitorizar novas ameaças;
- Permitir o fornecimento de serviços h-SOC mais simples e rápido, através da redução da dependência de terceiros que processam *malware* e análise forense.

Cláusula 38.ª

Capacidades de Resposta a Incidentes de Segurança

Deverá ser facultada total capacidade de resposta a incidentes de segurança, tais como:

a) Descoberta de Ativos: inventariação automática dos ativos de rede.

- i. A descoberta automática dos ativos de rede de dados deverá permitir ao h-SOC uma atualização real de quem está ligado ao sistema de informação, mesmo em ambientes que possuam alterações diárias (por ex., colaboradores que se liguem a rede de dados com PC's pessoais, máquinas fora do domínio, etc.);
- ii. As técnicas de scan da rede executada de forma ativa e passiva deverão permitir criar um inventário dos recursos instalados, um primeiro passo essencial para implementar com sucesso um programa de segurança abrangente;
- iii. Com um mapa da rede de dados completo e detalhado, o h-SOC poderá ter a visibilidade sobre a avaliação das vulnerabilidades, detetar e mitigar ameaças e monitorizar a rede e os serviços para análise de comportamentos estranhos e irregulares.

b) Avaliação de Vulnerabilidades: deteção de ativos que estão vulneráveis a ataques:

- i. A análise de vulnerabilidades deverá permitir a identificação de sistemas e aplicações vulneráveis, apoiando o h-SOC a priorizar as suas ações de remediação e a melhorar a postura de segurança da empresa, com base nas metodologias de resposta a incidentes orientadas para cada ameaça;
- ii. Ao combinar a descoberta de ativos com a avaliação das vulnerabilidades, a plataforma de gestão deverá ampliar a visibilidade da rede e a consciência de segurança, priorizando as ações a tomar;
- iii. O trabalho realizado pelo MSS internamente e externamente com base na integração dos log's das avaliações diárias sobre as quais a Porto Ambiente irá ser monitorizada sob diferentes vetores de ataque (XSS, RFI/LFI, Defacing, Land Attack, Fuzzing, entre outros), com recurso a bases de dados de

exploitation conhecidos e *zero-day* (desenvolvidos pelo h-SOC), permitirá ter uma visibilidade de 360° sobre a estrutura de dados da Porto Ambiente.

c) Detecção de Intrusões: Identificação de *hosts* alvo de ameaças ativas:

i. Deverá ser concebido e utilizado um sistema de deteção de intrusões na rede (IDS), através da instalação de sensores, de forma a permitir analisar o tráfego da rede para detetar ataques;

ii. O h-SOC deverá detetar ataques direcionados à rede de dados da empresa, nomeadamente a dispositivos vulneráveis de forma automática, no sentido de alertar o h-SOC para a ocorrência de tráfego malicioso na rede;

iii. Esta deteção deverá ser realizada em qualquer ponto da rede de dados e perímetro da rede, através do acesso aos *log's* e eventos de cada ativo que esteja no âmbito deste projeto (servidores, ativos de rede, antivírus, *firewalls*, bases de dados, aplicações críticas, etc.).

d) Bloqueio e mitigação de *malware*/intrusões: As ações de mitigação e bloqueio de diversos tipos de ataque deverão ser executadas sob metodologias específicas para cada tipo de ameaça:

i. Estas ações deverão ser realizadas em estreita coordenação com as equipas de TI da Porto Ambiente e das entidades que prestam serviço a esta entidade (desde operadores, serviços de suporte e manutenção, ...);

ii. Ataques como *ransomware*, fuga de informação, *botnets*, *malware* em smartphones, *defacement* de websites, *cryptocurrency*, *phishing*, *DDoS*, entre outros, deverão ser mitigados e bloqueados, cada um com processos específicos de resolução.

e) Monitorização comportamental e heurística: Identificação de alterações em condições de operação da rede consideradas normais:

- i. Deverão ser evidenciadas as alterações no comportamento da rede de dados, sistemas e serviços, de forma a indicar um ataque em execução ou um sistema comprometido;
- ii. Deverá ser promovida a combinação da análise de fluxo de rede (*NetFlow*) para ver mudanças no tráfego de rede, a captura de pacotes para análise forense, a monitorização dos serviços ativos para verificar proativamente as mudanças nos serviços e a coleta de *log's* para detetar anomalias reportadas por outros elementos da infraestrutura.

Cláusula 39.ª

Análise de Vulnerabilidades e Integração com o SOC

Deverá ser realizada uma análise de vulnerabilidades e integração com o SOC, nomeadamente através das seguintes ações:

- a) Recolha de Informação Passiva: nesta fase, deverão ser utilizados portais de internet especializados, motores de busca e redes sociais, de forma a recolher informação que possa vir a ser útil sobre os portais, serviços, tecnologias, colaboradores e/ou utilizadores, bem como outras ferramentas de obtenção passiva de informação;
- b) Recolha de Informação Ativa: nesta fase, deverão ser promovidos acessos diretos, não ofensivos, aos diversos portais e serviços online, de forma a melhor identificar e confirmar as tecnologias utilizadas. De acordo com as especificidades dos portais, deverão ser igualmente efetuados testes manuais, de forma a obter informação que escape a ferramentas automáticas;
- c) Identificação de vulnerabilidades no perímetro de segurança (DMZ), servidores e aplicações Web: após efetuado o levantamento de toda a informação de forma passiva e ativa, deverão ser efetuados testes customizados às tecnologias identificadas nos servidores e portais Web publicados internamente e externamente:

- i. Os pontos a testar vão depender do que for identificado nas fases de recolha de informação, bem como em resultados que surjam nesta mesma fase, mas de forma genérica deverão ser testadas, quando aplicável, vulnerabilidades *Cross Site Scripting (XSS)*, *Blind Structured Query Language Injection (Blind SQLi)*, *SQLi*, vulnerabilidades em *Procedural Language/Structured Query Language (PL/SQL)*, análise de vulnerabilidades *Remote File Inclusion (RFI)*, *Cookies*, *Javascript*, *Applets*, Código Flash, Certificados Digitais, *Fuzzing* (IP, TCP, UDP, cookies, forms, variáveis via URL encoding), entre outras que sejam aplicáveis à tecnologia utilizada pela empresa;
- d) Identificação de vulnerabilidades em outros serviços como SNMP/POP3/IMAP, NTP, VPN SSL/IPSEC, DNS, FTP, HTTP/HTTPS, entre outros: após efetuado o levantamento de toda a informação de forma passiva e ativa, deverão ser efetuados testes customizados aos serviços publicados pelos sistemas instalados na infraestrutura da Porto Ambiente;
- e) *Exploitation Zero-day/Zero-hour*: caso sejam descobertas vulnerabilidades e de forma a eliminar falsos positivos, deverá ser promovida uma simulação em laboratório em condições aproximadas, de forma a validar se se confirmam as falhas identificadas e qual a sua severidade:
 - i. Deverá ser desenvolvido código que demonstre a usabilidade das vulnerabilidades detetadas, caso não exista nenhum disponível publicamente quer em bases de dados na Internet, quer através de ferramentas *Open Source* e/ou comerciais;
- f) Injeção de Incidentes: sempre que seja confirmada alguma vulnerabilidade crítica, a empresa deverá ser prontamente informada, de forma a minimizar o tempo de exposição à falha de segurança:
 - i. As ferramentas a utilizar estão disponíveis em portais e exploits desenvolvidos pelo h-SOC, caso seja necessário. Os testes de intrusão serão

executados à medida que forem identificadas vulnerabilidades que permitam a sua execução, no sentido de validar se as vulnerabilidades são reais ou falsos positivos;

g) *Land Attacks* (Ataques *Denial of Service*): ataques à disponibilidade recorrendo a ferramentas de Negação de Serviços (*Denial of Service* - DoS) genéricas. Poderão ser utilizadas ou desenvolvidas ferramentas específicas, de acordo com possíveis vulnerabilidades que venham a ser detetadas, bem como realizados testes que serão coordenados previamente com a equipa de STI da Porto Ambiente.

Cláusula 40.ª

Funcionalidade e Benefício

No que respeita à resposta a incidentes de segurança, deverão ser promovidas as funcionalidades e respetivos benefícios que a seguir se indicam:

Funcionalidade	Benefício
Monitorização Comportamental e heurística	
Análise do <i>Network Flow</i> (NetFlow)	Fornecimento de uma visão ampla sobre o uso da largura de banda e aplicações em execução na rede
Captura de Pacotes	Captura de dados de pacotes para avaliar tráfego específico para análise detalhada de ameaças
Monitorização de Serviços Ativos	Certificação de que apenas os serviços que a Porto Ambiente necessita estão realmente ativos/em execução e não há interrupções indesejadas do serviço ou serviços que estejam em execução
Correlação de <i>log's</i>	Correlação de <i>log's</i> de infraestruturas locais/remotas, bem como de ferramentas/apps de terceiros para acelerar e simplificar a deteção de ameaças e sua correção/mitigação
Análise Forense	<i>Tracking</i> de ações de utilizadores, apps, com base nos <i>log's</i> que são encriptados e assinados digitalmente, recolha de artefactos e evidências, criando um relatório temporal de acontecimentos (fundamental protocolo NTP estar bem configurado em todos os ativos de rede e sistema)
Inteligência de Ameaças	
Integração de informação com base em <i>HoneyPots</i>	Através da simulação de falhas de segurança nos sistemas e recolha de informações sobre vetores de ataque com um share de informação ao nível internacional (<i>HoneyPot</i> não oferece nenhum tipo de proteção, apenas informação).

Cyberfeeds & Cyber Intelligence	Integração de Cyberfeeds/Intel, fontes de risco de todos os eventos ocorridos na Internet com info de alvos comprometidos (<i>compromised targets</i>), que possam comprometer a empresa.
Relatórios	
Por categorias, standards, ativos, <i>malware</i> , <i>users</i> , <i>apps</i> , ...	Standards ISO27001:2013, RGPD, ... e respetiva customização.

Cláusula 41.ª

Formação aos colaboradores

Deverão ser realizadas 2 (duas) ações de formação por ano, em formato *webinar*, para todos os colaboradores da empresa, cada uma com os seguintes módulos:

- Introdução à Segurança da Informação: Explicação da importância da segurança no contexto do dia a dia do colaborador;
- Introdução ao *phishing* - Fornecer uma visão breve, mas concisa, das práticas recomendadas relacionadas com a identificação e o tratamento de emails suspeitos;
- Evitar *links* perigosos - Dar aos colaboradores orientações práticas sobre como descobrir o destino real de um URL e examinar dicas visuais comuns que podem ajudar os colaboradores a determinar se um site é legítimo ou perigoso;
- Evitar anexos perigosos - Ajudar os colaboradores a entenderem por que devem tratar qualquer anexo de *email* como uma suspeita saudável e como lidar com este tipo de conteúdos;
- *Phishing* de entrada de dados - Explicar os perigos associados a formulários de entrada de dados maliciosos e ajudar os colaboradores a entenderem por que devem ser cautelosos com qualquer *email* que inclua uma solicitação de credenciais ou outras informações confidenciais;

- Ferramentas de proteção de email - Entender como proteger-se contra ataques de *phishing*, em combinação com ferramentas de proteção do serviço de email;
- Segurança do email em dispositivos móveis - Identificar e evitar emails de *phishing* em dispositivos móveis;
- Ameaças de *spear phishing* - Reconhecer e evitar ataques de *phishing* direcionados;
- Fundamentos de Segurança - Formação sobre os fundamentos da segurança informática. O colaborador irá perceber as ameaças e erros mais comuns na vida diária;
- Fundamentos de segurança em trabalho remoto - Reconhecer e evitar ameaças encontradas no trabalho realizado remotamente;
- Formação de URL – os colaboradores aprendem como examinar um URL, entender a origem do link e identificar URLs fraudulentos ou mal-intencionados;
- Segurança do email - os colaboradores aprendem a detetar técnicas de *phishing* em emails e a reconhecer links, anexos e informações falsificados;
- Segurança da Password – Os colaboradores recebem dicas e truques para criar passwords mais fortes, usar uma família de passwords para ajudar na recuperação da password e guardar passwords com segurança;
- Redes Sociais Seguras – Educar os colaboradores sobre tipos de “fraudes” que podem ser encontrados nos sites sociais, sobre implicações das redes sociais com informação demasiado exposta e sobre como detetar mensagens fraudulentas nas redes sociais;
- Proteger contra o *Ransomware* - Breve módulo de formação sobre como reconhecer e prevenir ataques de *ransomware*;
- Segurança de aplicações para dispositivos móveis - aprender a pesquisar componentes de aplicações e as implicações de permissões perigosas, que

podem ajudar a avaliar a confiabilidade e a segurança das aplicações móveis antes de efetuarem *download*;

- Segurança de dispositivos USB - Uma ameaça frequentemente negligenciada - os colaboradores precisam de estar cientes dos riscos associados às unidades USB e de outros equipamentos IoT alimentados por meio de portas USB;
- Segurança física - Aprender como evitar e corrigir violações de segurança física e obter as práticas recomendadas que ajudarão a manter pessoas, áreas e ativos seguros;
- Segurança além do escritório - educar os colaboradores a usar o Wi-Fi gratuito com segurança, os riscos do uso de computadores públicos e as proteções para equipamentos e informações da organização em casa e em viagem;
- Navegação segura na Web - Os colaboradores aprenderão a diferença entre o conteúdo do navegador e o conteúdo do site, como evitar *pop-ups* de vírus mal-intencionados, a importância de sair de sites, os riscos de formulários de preenchimento automático e identificar outros ataques comuns em sites;
- Engenharia social - Os colaboradores aprenderão a reconhecer táticas comuns de engenharia social, a criar defesas e a ter uma perceção sobre como os “engenheiros sociais” pensam;
- Informações Pessoais Identificáveis (PII) - Educar colaboradores sobre os diferentes tipos de PII, diretrizes para identificar, recolher e lidar com PII, ações a serem tomadas no caso de uma violação de PII e dicas e técnicas para melhorar a segurança geral de PI.

Cláusula 42.ª

Plano de Monitorização

O Plano de Fiscalização incluirá, designadamente, o seguinte:

- Acompanhamento em tempo real via acesso a um *Dashboard* para supervisão do projeto;

- Definição de políticas, métricas e fiscalização do projeto;
- Monitorização feita de forma integrada para equilibrar as operações diárias com o planeamento estratégico definido inicialmente no projeto;
- Informação aos parceiros e stakeholders;
- Informação aos colaboradores/funcionários da Porto Ambiente.

Cláusula 43.ª

Outros Deveres do Contraente Privado

O Contraente Privado deverá assumir, ainda, os seguintes deveres:

1. No caso de se verificar a indisponibilidade de algum dos consultores envolvidos no projeto, por razões planeadas (ex. férias) ou não planeadas (ex. doença), a equipa do Contraente Privado deverá garantir a substituição do mesmo por outro com competências técnicas e de gestão de projeto equivalentes.
2. O Contraente Privado responsabiliza-se por manter uma equipa coerente durante a duração do contrato, no sentido de dar continuidade ao serviço prestado e estabilidade à estratégia de gestão, minimizando os riscos de rutura de serviço.
3. Está contemplado o armazenamento/disponibilização de Logs pelo período máximo de 90 dias. Durante este período os Logs estarão disponíveis no SIEM.