

**AQUISIÇÃO DE SERVIÇOS PARA O CUMPRIMENTO DOS REQUISITOS DE SEGURANÇA E
RESPOSTA A INCIDENTES, IMPOSTOS PELO DL N.º 65/2021, DE 30 DE JULHO**

CADERNO DE ENCARGOS

PARTE I

CLÁUSULAS JURÍDICAS

Cláusula 1ª - OBJETO

O presente procedimento consiste na Aquisição de Serviços para o Cumprimento dos Requisitos de Segurança e Resposta a Incidentes, nos termos do Decreto-Lei n.º 65/2021, de 30 de julho, cuja especificação e atividades se encontra detalhado na Parte II – Cláusulas Técnicas do presente Caderno de Encargos.

Cláusula 2ª - PRAZO DE PRESTAÇÃO DO SERVIÇO E LOCAL DA EXECUÇÃO

Os serviços a prestar serão contratados por um período de 12 meses, após a assinatura do contrato.

Os serviços de assessoria podem ser prestados de forma presencial ou não presencial no âmbito das necessidades da CIM Viseu Dão Lafões.

Cláusula 3ª - PREÇO BASE

1- O preço contratual apresentado pelo concorrente contém todos os custos, encargos e despesas, cuja responsabilidade não esteja expressamente atribuída à CIM Viseu Dão Lafões, sendo o preço base fixado em 11.760,00 € (onze mil, setecentos e sessenta euros) que será acrescido do imposto sobre o valor acrescentado à taxa legal em vigor;

2- Serão excluídas as propostas, cuja análise revele o constante do nº 2 do artigo 70º CCP.

Cláusula 4ª - SANÇÕES CONTRATUAIS

Pelo incumprimento de obrigações emergentes do contrato, a CIM Viseu Dão Lafões pode exigir do prestador de serviços o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento nos seguintes termos:

- a) Pelo incumprimento dos prazos estabelecidos no cronograma apresentado pelo concorrente e aprovado pela CIM Viseu Dão Lafões, até 1% do preço contratual por cada semana de atraso.

Cláusula 5ª - CONDIÇÕES DE PAGAMENTO E FATURAÇÃO

1. O pagamento será efetuado a 60 (sessenta) dias após a receção das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. O Adjudicatário apresentará a fatura acompanhada de todos os elementos descritivos e justificativos que permitam a sua conferência.
3. Serão deduzidas, no pagamento a fazer ao Adjudicatário, as importâncias necessárias à liquidação das sanções contratuais que lhe tenham sido aplicadas.
4. Caso a fatura apresentada não mereça aprovação da Entidade Adjudicante, porque não esteja conforme com o contratado, esta comunicará tal decisão ao Adjudicatário que deverá apresentar outra em substituição, devidamente corrigida.

A fatura deverá incluir os seguintes elementos:

- Incidência do IVA, em separado;
- Emissão em nome da Comunidade Intermunicipal Viseu Dão Lafões.

Cláusula 6ª - SIGILO

1. O Adjudicatário garantirá o sigilo quanto a informações que os seus técnicos venham a ter conhecimento relacionadas com a atividade da Entidade Adjudicante.
2. O Adjudicatário deve limitar o acesso às informações confidenciais aos seus empregados, funcionários e contratados que tenham de recorrer às mesmas para correta execução do Contrato e assegurar que os mesmos são obrigados a manter essa confidencialidade nos termos em que esta é exigível ao Adjudicatário.
3. No final da execução do presente Contrato, o Adjudicatário entregará à Entidade Adjudicante todos os documentos por si utilizados ou preparados para a realização dos serviços prestados.

4. Todos os elementos documentais referidos no número anterior passarão a ser propriedade da Entidade Adjudicante sem prejuízo para direitos de autor e de direitos de propriedade industrial que o Adjudicatário ou qualquer sociedade em relação de grupo ou de domínio tenha sobre os mesmos.

5. Consideram-se excluídos das disposições anteriores:

- a) Os documentos e informações que sejam ou se tornem do conhecimento público, sem que o Adjudicatário de tal facto seja ou possa ser considerado direta ou indiretamente responsável;
- b) Os documentos e informações que estejam, no momento da sua comunicação, já em posse do Adjudicatário e não sejam objeto de restrições ou limitações;
- c) Os documentos e informações recebidos pelo Adjudicatário de Terceiros que não exijam ao Adjudicatário compromisso de confidencialidade.

Cláusula 7ª - CESSÃO DA POSIÇÃO CONTRATUAL

O Adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato.

Cláusula 8ª - RESPONSABILIDADE POR TERCEIROS

1. O Adjudicatário, salvo por dolo ou negligência não será responsável por qualquer incumprimento em que terceiros incorram a título de atraso, cumprimento defeituoso, ou incumprimento definitivo e seja qual for a natureza dos danos produzidos.

2. Sempre que o Adjudicatário sofra impedimentos na execução dos serviços para que foi contratado, em virtude de qualquer ato imputável a terceiros, deverá no prazo de 24 (vinte e quatro) horas, a contar da data de ocorrência, informar a Entidade Adjudicante de modo a esta ficar habilitada a tomar providências que estejam ao seu alcance. Em qualquer caso, o risco corre por conta do Adjudicatário.

Cláusula 9ª - CASOS FORTUITOS OU DE FORÇA MAIOR

1. Nenhuma das partes incorrerá em responsabilidade se por caso fortuito ou de força maior, designadamente greves ou outros conflitos coletivos de trabalho, for impedido de cumprir as obrigações assumidas no contrato.

2. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

Cláusula 10ª - REPRESENTANTES DO ADJUDICATÁRIO E DA ENTIDADE ADJUDICANTE

1. As relações de Entidade Adjudicante com o Adjudicatário processar-se-ão através de representante a designar pela Entidade Adjudicante. O Adjudicatário indicará, até 10 (dez) dias úteis após a adjudicação, o seu representante junto da entidade Adjudicante, com poderes para resolver a generalidade dos assuntos emergentes do Contrato.
2. A Entidade Adjudicante poderá fazer-se representar por assessores e/ou outras entidades de sua escolha, no acompanhamento da prestação de serviços.

Cláusula 11.ª - GESTOR DO CONTRATO

1. A CIM Viseu Dão Lafões deve designar um gestor de contrato para promover o devido acompanhamento permanente da execução do contrato, nos termos do previsto no artigo 290.º-A em conjugação com a alínea i) do n.º 1 do artigo 96.º, ambos do CCP, e que desempenhe o papel de interlocutor com a Parte contrária para todos os fins associados à execução contratual.
2. Caso o gestor do contrato detete desvios, defeitos ou outras anomalias na execução do contrato, deve comunicá-los de imediato ao órgão competente da CIM Viseu Dão Lafões, propondo, em relatório fundamentado, as medidas corretivas que se revelem necessárias.
3. A CIM Viseu Dão Lafões designa como gestor do contrato, Carina Andreia Rodrigues dos Santos, a qual pode, no decurso da prestação de serviços, solicitar esclarecimentos atinentes à mesma.

Cláusula 12ª - PESSOAL

1. É da responsabilidade do Adjudicatário a seleção e o recrutamento de todo o pessoal especializado, não especializado e auxiliar para a direção e a execução da sua prestação de serviços, assim como todos os encargos e despesas com esse pessoal, nomeadamente, de viagem, alojamento, alimentação, deslocações diárias, ajudas de custo, subsídios diversos, etc.

2. O recurso a horas suplementares, ou trabalho em dias feriado ou de descanso semanal, por parte do pessoal do Adjudicatário, são do seu encargo, não podendo ser faturado à Entidade Adjudicante, com exceção de solicitação expressa e fundamentada da Entidade Adjudicante e em caso de ocorrência de força maior, nos termos em que se encontra fixada no presente Caderno de Encargos.
3. O Adjudicatário é obrigado a manter nos locais de trabalho, a disciplina e boa ordem do pessoal ao seu serviço.

Cláusula 13ª - SUBCONTRATADOS E TAREFEIROS

1. A responsabilidade pela execução de todos os serviços prestados e contratados será sempre do Adjudicatário e só dele, o qual deverá submeter, com a Proposta, as empresas com quem venha a subcontratar a execução de parte dos serviços que constituem a presente prestação.
2. Caso se verifique a necessidade de o Adjudicatário recorrer, por razões de natureza excecional, à subcontratação ou execução de tarefas por Terceiros, requererá, para os casos em que tal não esteja claramente indicado na sua Proposta, prévia autorização à Entidade Adjudicante, fazendo acompanhar esse pedido dos elementos comprovativos da necessidade invocada e da capacidade e competência do Subcontratado ou Tarefeiro que propõe, sendo os eventuais atrasos derivados de autorização exclusivamente imputáveis ao Adjudicatário.

Cláusula 14ª - PATENTES, LICENÇAS E MARCAS REGISTRADAS

1. São da responsabilidade do Adjudicatário quaisquer encargos decorrentes da utilização, no fornecimento, de marcas registadas, patentes registadas ou licenças.
2. Caso a Entidade Adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o Adjudicatário indemniza-o de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.
3. O Adjudicatário é responsável por qualquer violação das normas legais ou direitos de terceiros em relação a patentes, modelos de utilidade, marcas, modelos e desenhos industriais direitos de

autor ou direitos conexos, bem como quaisquer direitos de propriedade intelectual por ele utilizados, em que incorra no âmbito do presente Contrato.

Cláusula 15ª - RESOLUÇÃO DO CONTRATO

1. O incumprimento do Contrato por qualquer das Partes contratantes dará, à Parte não faltosa, o direito de o resolver nos termos gerais do direito.
2. Para efeitos do número anterior, a Entidade Adjudicante notificará por escrito o Adjudicatário para sanar as deficiências assinaladas no prazo de 5 (cinco) dias úteis.
3. Não se verificando sanadas as deficiências notificadas, a Entidade Adjudicante poderá resolver então o contrato, operando-se a resolução na data da receção da referida notificação.
4. O incumprimento do prazo para a prestação de serviços dá direito à Entidade Adjudicante de proceder à resolução automática do presente contrato operando-se esta resolução na data de receção da notificação por parte do Adjudicatário.
5. Com a receção da notificação o Adjudicatário deve iniciar, de imediato, todas as diligências que lhe permitam cessar a prestação de serviços.
6. Caso a Entidade Adjudicante venha a resolver o Contrato, o Adjudicatário deverá indemnizar a Entidade Adjudicante pelo valor dos danos e prejuízos a este causados em virtude do comportamento faltoso.
7. A resolução do Contrato, por qualquer razão, não prejudicará ou afetará os direitos constituídos e os deveres e responsabilidades assumidas por qualquer dos outorgantes.

Cláusula 16ª - FORO COMPETENTE

1. No caso de divergência relativo à interpretação, execução ou cumprimento de obrigações emergentes do presente Contrato, os Outorgantes, obrigam-se a procurar uma solução consensual.
2. Qualquer litígio ou diferendo será submetido à apreciação dos responsáveis máximos dos Outorgantes, que envidarão todos os esforços para obter uma solução consensual.

3. Se no prazo de 30 dias após o início da situação de diferendo, se frustrar a tentativa de resolução referida no número anterior, o litígio ou diferendo será decidido por recurso ao Tribunal Administrativo e Fiscal de Viseu, com renúncia expressa a qualquer outro.

Cláusula 17ª - PREVALÊNCIA

1. Fazem parte integrante do contrato o caderno de encargos, a carta convite e a proposta do Adjudicatário.
2. Em caso de dúvidas aplicam-se as regras de prevalência definidas pelos números 5 e 6 do artº 96º do CCP.

Cláusula 18ª - 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 19ª - LEGISLAÇÃO APLICÁVEL

A tudo o que não esteja especialmente previsto aplica-se o regime previsto no CCP e demais legislação aplicável.

PARTE II

CLÁUSULAS TÉCNICAS

Especificações Técnicas

Cláusula 20ª – DESCRIÇÃO

A presente prestação de serviços deverá incluir todas as atividades e procedimentos necessários ao total cumprimento dos requisitos de segurança e resposta a incidentes, impostos à CIM Viseu Dão Lafões pelo Decreto-Lei n.º 65/2021, de 30 de julho.

Deverá ser adotada uma metodologia de implementação, devidamente adequada e apoiada em 6 grandes fases, conforme descrito seguidamente:

FASE 1 – Diagnóstico

A avaliação da Fase 1 (Diagnóstico) deverá contemplar o seguinte universo geral de atividades para avaliação do SGSI (Sistema de Gestão de Segurança da Informação) da CIM Viseu Dão Lafões:

- Levantamento de situações anómalas (algumas delas poderão ser repetidas);
- Levantamento de políticas, processos e procedimentos de segurança e resposta a incidentes de segurança;
- 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);
- Recolha e monitorização de informação da estrutura IT da CIM Viseu Dão Lafões, bem como questões realizadas a indivíduos com diferentes graus de responsabilidade na sua estrutura funcional. Execução feita com base no Checklist Information Security Management BS ISO/IEC 27001:2013;
- Recolha das configurações de switching e routing (layer 2 e 3) para análise das metodologias de segurança utilizadas pela CIM Viseu Dão Lafões ao nível de networking;
- Recolha de informação sobre a arquitetura e tecnologias utilizadas em toda a estrutura IT, com principal ênfase na DMZ;
- Identificação e análise dos ativos de rede;
- Identificação dos servidores (independentemente do sistema operativo) para verificação de GPOs, portas/protocolos e serviços disponibilizados.

Nesta fase deverão ainda ser verificados os seguintes controlos de área, com base nas ISO 27001:2013 e 27005, e desde que aplicáveis à CIM Viseu Dão Lafões:

- Políticas de segurança da informação;
- Organização da segurança da informação;
- Segurança dos Recursos Humanos;
- Gestão de Ativos;

- Gestão e controlo de acessos à CIM Viseu Dão Lafões;
- Criptografia;
- Segurança física e ambiental;
- Segurança das operações;
- Segurança das comunicações;
- Aquisição de sistemas, desenvolvimento e manutenção;
- Relação com fornecedores;
- Gestão de incidentes de segurança da informação;
- Aspetos da segurança da informação na continuidade de negócio;
- Compliance.

FASE 2 – Resposta a Incidentes de Segurança

Nesta fase serão desenvolvidos e implementados todos os procedimentos necessários à criação das respostas adequadas a incidentes de segurança. Para tal, deverão ser considerados os seguintes critérios:

- Implementação de contramedidas;
- Monitorização em tempo real e análise da triagem/incidente;
- Análise de vulnerabilidades e Penetration Testing (PENTEST);
- Resposta a incidentes no local;
- Mapeamento de rede/Vulnerability Scanning;
- Ferramentas de engenharia;
- Tuning dos sensores;
- Coletar, reter e armazenar dados da auditoria/criação e gestão de conteúdos de auditoria.

FASE 3 – Obrigações decorrentes do DL 65/2021

Para além das medidas técnicas e organizativas que terão de ser implementadas e geridas, deverão ainda ser cumpridas as obrigações decorrentes do imposto pelo Decreto-Lei n.º 65/2021.

Nesta fase deverá proceder-se à:

- Identificação do “Ponto de Contacto Permanente” da CIM Viseu Dão Lafões;
- Identificação do “Responsável de Segurança”;
- Identificação de funções ou atividades críticas da CIM Viseu Dão Lafões;
- Estabelecimento de canais de comunicação;
- Análise de risco;
- Definição da cadeia de risco;
- Criação ou adaptação da “Política de Segurança de Informação”, atendendo à realidade da CIM Viseu Dão Lafões;

- Finalização dos procedimentos de notificação de incidentes (iniciados na fase anterior).
- Tendo em conta que se deverá elaborar o plano de segurança, este ocorrerá na fase da implementação.
- Criação do “Relatório Anual” para a CIM Viseu Dão Lafões e do respetivo “Inventário de Ativos” conforme estabelecido no DL65/2021.

FASE 4 – Desenvolvimento da Arquitetura de Segurança

Nesta fase pretende-se desenvolver as ações que permitirão dotar a CIM Viseu Dão Lafões com os principais recursos processuais e técnicos essenciais para a defesa eficaz dos seus ativos, quer a nível de perímetro de rede, quer dos servidores, postos de trabalho e outros dispositivos.

Deverão ser executadas as seguintes ações:

- Desenho e implementação da arquitetura e segurança perimétrica (caso se aplique);
- Implementação do sistema de recolha e armazenamento do fluxo de tráfego;
- Comunicação com o CNCS;
- Inventariação de ativos / produção de um mapa de redes;
- Verificação da recolha centralizada de registos (logs);
- Criação de instrumentos de correção ou mitigação de incidentes;
- Conformidade com a legislação aplicável e normas da área de atividade;
- Criação de uma Política de Uso Aceitável (PUA);
- Manutenção de infraestruturas de cópias de segurança e reposição (backup/restore);
- Realização de, pelo menos, duas ações de awareness/formação/ano na CIM Viseu Dão Lafões, destinadas a todos os colaboradores (30), em áreas como: evitar ataques de phishing, links perigosos, anexos, cuidados com o trabalho remoto, segurança no serviço de email, password, redes sociais, entre outros módulos.

FASE 5 – Implementação

A fase de implementação deverá incluir a realização de auditorias de segurança e a adoção de mecanismos de supervisão, assim como a consolidação de informação de registo e monitorização no sistema integrado de gestão de eventos (SIEM), ou seja:

- Definição de procedimentos de operação;
- Instalação e configuração de um Security Information and Event Management (SIEM);
- Plano de segurança;
- Auditoria de segurança a bases de dados;
- Mecanismos de monitorização;
- Hardening das configurações;
- Simulacros de incidentes de cibersegurança;

- Definição de procedimentos de reação a incidentes;
- Testes de aceitação de serviços e mecanismos honeypots;
- Resposta a incidentes de segurança.

FASE 6 – Formação

A formação dos colaboradores da CIM Viseu Dão Lafões ocorrerá, pelo menos, duas vezes, em datas a definir no contexto do plano de projeto, e durante o prazo previsto para a prestação dos serviços.

A fase de formação incluirá todos os colaboradores da instituição, e considerará os seguintes conteúdos/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 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 com 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 auxiliar os colaboradores a assumir uma postura cautelosa perante emails que incluam 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 reconhecer links, anexos e informações falsificados.
- Segurança da Password: Os colaboradores aprendem técnicas 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, implicações das redes sociais com informação demasiado exposta e 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 ajudá-los 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 estar cientes dos riscos associados às unidades USB e de outros equipamentos IoT alimentados por meio de portas USB.
- Segurança física: Aprender a evitar e a 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 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 PII.

Cláusula 21ª – CRONOGRAMA/PLANEAMENTO DE ATIVIDADES

A presente prestação de serviços deverá incluir todas as atividades, procedimentos e produção de entregáveis necessários ao total cumprimento dos requisitos de segurança e resposta a incidentes, impostos à CIM Viseu Dão Lafões pelo Decreto-Lei n.º 65/2021, de 30 de julho.

Deverá ser apresentado um cronograma de execução do projeto, incluindo a descrição das atividades, entregáveis/resultados esperados, bem como a respetiva duração, considerando, no mínimo, os itens apresentados no quadro seguinte.

Descrição	Dependências	Entregáveis	Duração Total (dias)
Arranque do Projeto	Disponibilidade de um recurso com know-how geral das Apps / sistemas para acompanhamento do projeto.	Briefing Inicial do projeto pelo Gestor / Auditor do projeto; Plano de Trabalhos Inicial	
ISO27K			

Descrição	Dependências	Entregáveis	Duração Total (dias)
A.5 - Políticas de Segurança da Informação	. Identificação do responsável da segurança . Identificação de funções ou atividades críticas . Estabelecimento de canais de comunicação . Análise de risco . Cadeia de responsabilidade . Política de segurança . Procedimentos de notificação de incidentes . Recolha das configurações de switching e routing (layer 2 e 3) para análise das metodologias de segurança utilizadas.	. Definição da cadeia de responsabilidade, podendo a mesma ser ajustada ao longo de todo o processo . Definição dos privilégios de acesso individual, tendo em conta as funções desempenhadas e as responsabilidades inerentes . Criação da Política de Segurança de Informação adequada à organização em concreto, atendendo às suas necessidades e responsabilidades . Elaboração de um procedimento de notificação de incidente de cibersegurança, com impacto nas funções ou atividades identificadas como críticas. . Resultado da análise de conformidade com a legislação aplicável e normas da área de atividade. . Criação de uma política de uso aceitável (PUA) . Elaboração de plano de segurança, contendo a política de segurança, descrição das medidas organizativas, etc.	
A.6 - Organização da Segurança da Informação			
A.7 - Segurança dos Recursos Humanos			
A.8 - Gestão de Ativos			
A.9 - Controlo de Acessos			
A.10 - Criptografia			
A.11 - Segurança Física e ambiental			
A.12 - Segurança das Operações			
A.13 - Segurança das comunicações			
A.14 - Aquisição de sistemas, desenvolvimento e manutenção			
A.15 - Relação com fornecedores			
A.16 - Gestão de incidentes de segurança da informação			
A.17 - Aspectos da segurança da informação na continuidade de negócio			
A.18 - Compliance			
PTES			
Pre-engagement Interactions	. Tecnologias, sistemas (configurações, fabricantes), Recursos Humanos; . Arquitetura de rede e sistema instalados / em operação . Arquitetura aplicacional, frameworks e BDs; . Tecnologias, sistemas (configurações, fabricantes); . Arquitetura de rede e sistema instalados / em operação;	. Desenho e implementação da arquitetura e segurança perimétrica . Será elaborado/atualizado uma inventariação de ativos . Criação de mecanismos proporcionais ao risco existente de eliminação ou corrupção de dados, em sistemas que são importantes para o bom funcionamento da organização. . Auditorias de segurança às bases de dados da	
Intelligence Gathering			
Threat Modeling			

Descrição	Dependências	Entregáveis	Duração Total (dias)
Vulnerability Analysis	. Desenho da base de dados, das aplicações e arquitetura de comunicação, níveis de acessos e interligações; . Coordenação da injeção de incidentes (ataques DoS, RFI/LFI, Fuzzing,...) com a equipa de TI; . Identificação do IP público a partir do qual serão injetados incidentes de segurança.	organização. . Realização de robustecimento dos sistemas, alinhado com o mapeamento das ameaças, ações de mitigação dos riscos e com a execução das atividades corretivas.	
Avaliação das propriedades ACID (Atomicidade, Consistência, Isolamento e Durabilidade)			
Testes de benchmark TPC-C[1]			
Avaliar o modelo de dados (sql schema)			
Avaliar a framework aplicacional			
Vulnerability Analysis			
Exploitation			
Post Exploitation			
Reporting			
Resposta a incidentes (implementação + ongoing)			
Setup SIEM	. Verificação da recolha da informação de registo (logs) e periodo de armazenamento dos mesmos, providenciando a monitorização aos principais portais. . Recolha de informação sobre a arquitetura e tecnologias utilizadas em toda a estrutura IT, com principal ênfase na DMZ; . Identificação e análise dos ativos de rede; . Identificação dos servidores (independentemente do sistema operativo) para verificação de GPOs, portas/protocolos e serviços disponibilizados	. Implementação um sistema de recolha do fluxo de tráfego . Implementação de procedimento de comunicação entre a organização e o CNCS . Criação de instrumentos de correção ou mitigação de incidentes . Identificação dos procedimentos para a deteção de incidentes, atualização de ativos, triagem, análise de observáveis, fluxo de informação interno e de interação com entidades externas . Instalação e configuração de um sistema de monitorização . Apoio ao sistema de gestão e correlação de dados e eventos, por forma a facilitar a análise em tempo real e acelerando a tomada de ações defensivas . Realização de um simulacro de incidente de cibersegurança para avaliação da organização	
Tunning dos Sensores			
Mapeamento de Rede / Vulnerability Scanning			
Monitorização em Tempo Real e Análise da Triagem / Incidente			
Vulnerability Analysis Coletar, Reter e Armazenar dados da Auditoria/ Criação e Gestão de Conteúdos de Auditoria			
Implementação de Contramedidas			
Resposta a Incidentes no Local			

Descrição	Dependências	Entregáveis	Duração Total (dias)
Ferramentas de Engenharia			
Formação & Awareness			
Ministrar os módulos de formação/Awareness conforme ponto 12.6 desta proposta	. Validação dos módulos de formação a ministrar, enquadramento com as políticas de segurança da informação.	. Aquisição de conhecimentos de segurança no sentido lato.	
(2 ações / semestre)	. Coordenação com o RH da organização dos grupos e horários	. Abordagem prática de técnicas de phishing e similares para comprometer os dados pessoais e da organização.	
Projeto ISO 27k + PTES + SOC + Formação			

Cláusula 22ª - CONTROLO DE QUALIDADE

Não serão aceites quaisquer elementos ou informações que não respeitem as condições constantes nas Peças do Procedimento deste Ajuste Direto.