



INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP

CADERNO DE ENCARGOS

Concurso Público sem publicação no JOUE N° 2021210/157

Aquisição de Serviços de Auditoria de segurança de informação no Centro de dados do IEFP, IP



PARTE I CLAÚSULAS JURÍDICAS

Cláusula 1.ª

Objeto

O presente concurso tem por objeto a aquisição de serviços de auditoria de segurança de informação à rede informática do IEFP, IP, sob a forma de testes de intrusão e de serviços de consultoria para avaliação do estágio de maturidade dos controlos técnicos implementados, com o objetivo de identificar potenciais vulnerabilidades e recomendações associadas respetivamente às suas infraestruturas, sistemas e aplicações, enquadradas no Regulamento Geral de Proteção de Dados (RGPD) e Resolução de Conselho de Ministros (RCM) nº 41/2018.

Cláusula 2.ª

Local da prestação dos serviços

Os serviços, alvo do presente concurso, serão prestados nas instalações dos Serviços Centrais do IEFP, IP, localizadas na Rua de Xabregas, n.º 52, em Lisboa e nas instalações de 1 Serviço de Emprego e de 1 Serviço de Formação da área da Grande Lisboa.

Cláusula 3.ª

Duração do contrato

A prestação de serviços terá início com a assinatura do contrato, tendo a duração de 8 meses, com uma duração estimada de 75 dias de trabalho efectivos.

Cláusula 4.ª

Preço base

O preço preço base para os serviços a prestar é de 60 000,00€ (sessenta mil euros), acrescido de IVA à taxa legal em vigor.

Cláusula 5.ª

Condições e prazos de pagamento

1. A(s) quantia(s) devida(s) pelo IEFP.I.P., nos termos da cláusula anterior, deve(m) ser paga(s) no prazo de 30 (trinta) dias após a receção pelo IEFP, I.P, das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. As faturas serão enviadas para a Direção de Serviços de Gestão Administrativa e Financeira, sita na Rua de Xabregas, 52, 1949-003 Lisboa, com o discriminativo das atividades desenvolvidas durante o período faturado, e acompanhadas dos documentos justificativos, se necessário.



3. Em caso de discordância por parte do IEFP, I.P., quanto aos valores indicados nas faturas, deve este comunicar ao prestador de serviços por correio eletrónico, os respetivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. Na eventualidade do não cumprimento do prazo de pagamento referido, aplicar-se-á o previsto na Lei nº 3/2010, de 27 de abril, que estabelece a obrigatoriedade do pagamento de juros de mora, calculados à taxa legal em vigor.
5. O pagamento de quaisquer valores apresentados apenas será efetuado após aceitação dos serviços, a que se referem esses valores.
6. O Plano de Facturação previsto será o seguinte:
 - a) 25% após início dos trabalhos;
 - b) 25% com o fim da fase de testes (com entrega relatório);
 - c) 20% com o fim da 1ª fase de retestes;
 - d) 20% com o fim da 2ª fase de retestes (com entrega relatório);
 - e) 10% com a aceitação final do projecto por parte do IEFP.
7. De acordo com a Diretiva 2014/55/EU e Decreto-Lei 123/2018, de 28 de dezembro, a partir de 18 de abril de 2020 o Primeiro Outorgante fica obrigado a receber faturas eletrónicas no modelo a que se refere o n.º 3 do artigo 299.º-B do Decreto-Lei 111-B/2017 de 31 de agosto, estando o IEFP vinculado à plataforma de faturação eletrónica da ESPAP – FE-ESPAP.

Cláusula 6.ª

Obrigações do adjudicatário

1. O adjudicatário obriga-se a prestar os serviços ao IEFP, IP, nos termos das disposições do presente caderno de encargos, de acordo com a respetiva proposta e com as orientações e recomendações técnicas recebidas.
2. O adjudicatário fica obrigado a colocar ao dispor da entidade adjudicante todos os recursos alocados e de acordo com os perfis indicados, no prazo de 15 dias após a assinatura do contrato, sob pena de resolução do contrato
3. Sem prejuízo do referido no número anterior constituem, designadamente, obrigações do adjudicatário:
 - a) Obrigação de elaboração de relatórios referentes à prestação dos serviços, quando solicitado pelo IEFP, IP.;
 - b) Obrigação de prestação de informação e/ou esclarecimentos, relativamente aos serviços e ao cumprimento das obrigações emergentes do contrato, quando solicitado pelo IEFP, IP, e com a periodicidade que for julgada necessária;
 - c) A obrigação prevista na alínea anterior compreende o dever de o adjudicatário participar em reuniões com o IEFP, IP, ou com que este vier a designar;
 - d) Obrigação de submissão a fiscalização por parte do IEFP, IP, ou outra entidade que este designar;
 - e) Obrigação de substituição de qualquer elemento da equipa de Projeto, mediante solicitação fundamentada do IEFP, IP.



Cláusula 7ª

Cessão da posição contratual por incumprimento do cocontratante

1. Em caso de incumprimento total ou parcial das obrigações a que o cocontratante se obriga e que sejam geradoras de resolução do contrato, deverá o mesmo ceder a sua posição contratual ao concorrente do procedimento pré contratual pela ordem sequencial, de acordo com a classificação final obtida para a adjudicação da conclusão dos trabalhos.
2. A execução do contrato ocorrerá nas mesmas condições já propostas pelo cedente no procedimento pré contratual original.
3. A cessão da posição contratual opera nos termos definidos no artigo 318-A do Código dos Contratos Públicos.

Cláusula 8ª

Casos Fortuitos ou de Força Maior

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.

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 9ª

Outros encargos

Correm por conta do adjudicatário as despesas inerentes à elaboração da proposta, bem como quaisquer despesas derivadas da prestação das cauções e as inerentes à celebração do contrato.

Cláusula 10ª

Obrigações de sigilo

O adjudicatário obriga-se ao sigilo de quaisquer informações que obtenha em virtude da execução do contrato, pelo período de 5 anos, salvo se prévia e expressamente autorizado pela entidade adjudicante, nos termos e para os efeitos da Lei de proteção de Dados Pessoais.

Cláusula 11ª

Dados pessoais

1. Os Outorgantes comprometem-se a respeitar o Regulamento Geral de Proteção de Dados (RGPD) em vigor e demais legislações nacionais aplicáveis aos dados pessoais.
2. O Primeiro Outorgante enquanto responsável pelo tratamento dos dados fornecidos, informa que os mesmos serão utilizados para garantir a adequada execução do contrato, nomeadamente identificação do Segundo Outorgante e faturação ao abrigo do Código dos contratos Públicos.



INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP

3. Os dados pessoais fornecidos serão conservados apenas durante o período de execução do contrato, podendo ser mantidos de acordo com as exigências legais inerentes à finalidade do tratamento para que foram recolhidos.

Cláusula 12.^a

Cessão da posição contratual

1. O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da entidade adjudicante.
2. Para efeitos de autorização prevista no número anterior, deve ser apresentada pelo cessionário toda a documentação exigida ao adjudicatário no presente procedimento.

Cláusula 13.^a

Subcontratação

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

Cláusula 14.^a

Outras obrigações

Sem prejuízo de outras obrigações previstas na legislação aplicável, no Caderno de Encargos ou nas cláusulas contratuais da celebração do Contrato decorrem para o Adjudicatário as seguintes obrigações principais:

- a) Entregar toda a documentação necessária à adjudicação, no prazo de 10 dias após a notificação de adjudicação, nomeadamente:
 - i) Declaração emitida conforme Modelo constante do Anexo II do Programa do Concurso;
 - ii) Documento comprovativo que não se encontra nas situações previstas nas alíneas b), d), e) e h) do Artigo 55.º do Decreto-Lei nº 18/2008, de 29 de janeiro.
- b) A título acessório, o Adjudicatário 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 apropriado à perfeita e completa execução das tarefas a seu cargo.

Cláusula 15.^a

Gestor de Contrato

Nos termos e para o efeito do disposto no artigo 290º-A do CCP, irá ser designado um gestor de contrato.



Cláusula 16º

Responsabilidade do Adjudicatário

O adjudicatário responde pelos danos que causar à entidade contratante em razão do incumprimento culposos das obrigações que sobre ele impendam.

O adjudicatário responde ainda perante a entidade contratante pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações assumidas, como se tais atos ou omissões fossem praticados por aquele.

Cláusula 17ª

Despesas

Correm por conta do adjudicatário, todas e quaisquer despesas, nomeadamente as de deslocação e estadia, em que este haja de incorrer em virtude da execução das obrigações que para aquele emergem do presente Cadernos de Encargos e do contrato.

Cláusula 18º

Prevalência

Fazem parte integrante da relação contratual o Caderno de Encargos, os esclarecimentos e a Proposta do Adjudicatário.

Em caso de dúvida prevalece em primeiro lugar o Caderno de encargos, seguidamente os esclarecimentos e por último a Proposta do Adjudicatário.

Cláusula 19º

Lei Aplicável

O contrato rege-se pela lei portuguesa.

Cláusula 20º

Foro Competente

Para todas as questões emergentes do contrato será competente o Tribunal de Jurisdição Administrativa com sede em Lisboa.



CLÁUSULAS TÉCNICAS

CARACTERÍSTICAS DA PRESTAÇÃO DE SERVIÇOS

Cláusula 21.^a

Objeto

No âmbito das suas funções, o IEFP, IP depende dos seus sistemas de informação para a prestação dum serviço de qualidade ao cidadão. Desta forma é essencial que, dada a sua criticidade, estes sistemas estejam, em termos de segurança, protegidos de qualquer ameaça que coloque em causa o seu bom funcionamento e que, eventualmente, coloque em causa a segurança da rede do IEFP, IP tornando-a vulnerável a ataques informáticos.

Por outro lado, urge dar resposta a uma obrigatoriedade legal, que consiste na implementação do estabelecido na Resolução de Conselho de Ministros nº 41/2018, que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais.

Neste sentido, pretende-se efetuar uma aquisição de serviços para:

- i) Elaboração de testes de intrusão com vista à deteção de vulnerabilidades de segurança nas vertentes de Infraestruturas (Sistemas), Redes e Aplicações informáticas;
- ii) Consultoria de apoio à resolução das vulnerabilidades detetadas.

Cláusula 22.^a

Calendarização e planificação dos trabalhos

A calendarização dos trabalhos é definida consoante as necessidades do IEFP, IP.

Cláusula 23.^a

Horário de trabalho

1. Os serviços de acordo com o exposto na clausula 1^a, deverão ser efetuados nos Serviços Centrais do IEFP, IP, num Serviço de Emprego e num Serviço de Formação, a definir, na área da grande Lisboa, em conformidade com o acordado com a entidade adjudicante, no horário normal de funcionamento da mesma, das 9h00 às 18h00. Em virtude da situação pandémica em que vivemos os mesmos poderão excepcionalmente vir a ser executados de forma remota, no entanto esta situação deverá ser sempre ser alvo de aprovação prévia por parte do IEFP, IP.
2. Caso se verifique a necessidade de efetuar trabalho fora do período definido no número anterior, incluindo fins de semana e feriados, o adjudicatário deverá disponibilizar recursos para o efeito, sem quaisquer custos adicionais para o IEFP, IP.



INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP

3. Para todos os efeitos previstos no presente caderno de encargos, cada dia de trabalho corresponde a um período de 8 (oito) horas efetivas de trabalho.

Cláusula 24.^a

Logística e ferramentas de suporte

1. Caberá ao IEFP assegurar:
 - a) Instalações adequadas ao desenvolvimento dos serviços objeto de contrato;
 - b) Pontos de acesso à Intranet;
 - c) Serviços de impressão;
2. Todos os restantes aspetos logísticos, nomeadamente, telemóveis, computadores, e quaisquer ferramentas informáticas de suporte ao desenvolvimento dos trabalhos, bem como, todos os encargos relativos a despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais, serão da responsabilidade do adjudicatário.

Cláusula 25.^a

Níveis de serviço

1. O adjudicatário, no que respeita à prestação dos Serviços, e no decurso da sua intervenção acordada com o IEFP, IP, se provocar uma anomalia no correto funcionamento no sistema intervencionado, deverá proceder à sua resolução dentro dos prazos abaixo indicados:
 - a) Prioridade Crítica – inoperabilidade do sistema – 2 horas (este nível de serviço pressupõe a resolução do problema igualmente dentro do período máximo de 2 horas);
 - b) Prioridade Alta – mapas ou processos críticos para a entrega de requisitos legais ou operacionais – 4 horas;
 - c) Prioridade Média – mapas ou processos críticos para a entrega de requisitos legais ou operacionais com data planeada de entrega – 1 dia;
 - d) Prioridade Baixa – Melhorias ao sistema atual – 5 ou mais dias.
2. Nas intervenções programadas, uma vez analisado(a) o(a) pedido/questão em causa, o adjudicatário deverá apresentar, por escrito, uma estimativa do esforço necessário para a sua resolução.
3. A estimativa então apresentada deverá ser objeto de análise e concordância expressa por parte do IEFP.

Cláusula 26.^a

Penalidades

Caso o adjudicatário não cumpra, por causa que lhe seja imputável, os níveis de serviço definidos na cláusula, poderá ser aplicada uma penalidade, calculada de acordo com a seguinte fórmula:

$$P=(VxA) \times 0,6, \text{ em que}$$



INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP

P = montante da penalidade;

V = o custo por hora de um técnico a tempo inteiro;

A = número de horas em atraso.

PARTE III

CLÁUSULAS TÉCNICAS ESPECÍFICAS

Realização de testes de intrusão ao Parque de servidores e estações de trabalho do IEFP, IP

Cláusula 27.^a

Âmbito

O IEFP, IP presta um conjunto de serviços ao cidadão assentes em sistemas críticos e vitais para a sua atividade, residentes no Centro de Dados Principal em Xabregas, e como forma de garantir o cumprimento das suas práticas de gestão tecnológica, pretende efetuar a contratação de serviços de auditoria com vista à redução do risco, na ótica da Segurança da Informação.

Desta forma, pretende-se sejam efetuados Testes de intrusão, cujo objetivo consiste numa avaliação pontual dos sistemas informáticos do IEFP, IP, consubstanciada na identificação e acompanhamento das vulnerabilidades e do risco associado, definindo estratégias e meios para a sua mitigação.

Os serviços de auditoria de segurança serão efetuados nos servidores de suporte às aplicações Core do IEFP, IP (Sigae, SGFor, Sigofa/SIFGo, SGD, IEFPOnLine e NetForce, entre outras) e, por amostragem, em 10% das estações de trabalho dos Serviços Centrais e das Unidades Orgânicas Locais de todo o País, sendo obrigatória a realização dos referidos testes, de forma presencial, num Serviço de Emprego e num serviço de Formação da área da grande Lisboa. Esta prestação de serviços deverá ter uma duração estimada de **75 dias úteis**, repartidos da seguinte forma:

- 40 dias de testes de intrusão iniciais (inclui elaboração de relatório final da fase de testes);
- 10 dias de testes de intrusão intermédios (retestes), para verificação das vulnerabilidades já corrigidas;
- 10 dias de testes finais (retestes) para verificação do estado dos sistemas envolvidos, e consequente balanço final de segurança (inclui elaboração de relatório final de projecto);
- 15 dias para apoio à eventual resolução de problemas de segurança detetados (bolsa de horas).

Cláusula 28.^a

Tipos de intervenção

1. O IEFP, IP poderá requisitar ao adjudicatário os seguintes tipos de intervenção, que compreendem, entre outras, as seguintes tarefas:

- a) Realização de Testes de Intrusão de acordo com o âmbito definido;



- b) Realização do tipo de testes que se incorporam nas categorias descritas nos apêndices 1, 2 e 3, não esgotando estas propostas, de modo algum, a multiplicidade de situações que enfrentarão, devendo ser considerada a realidade do IEFP em avaliação - tecnologia e serviços, identificando outros testes que se considerem mais adequados;
- c) São pretendidos os seguintes trabalhos de auditoria:
- i. Pretende-se a realização de testes de avaliação da segurança informática conforme as categorias referidas no apêndice 1, entre outras, incluindo-se ainda a validação de vulnerabilidades que tenham sido identificadas em auditorias anteriores (O IEFP, IP Informará das mesmas na fase inicial de projecto);
 - ii. Identificar vulnerabilidades das infraestruturas, conforme as categorias referidas no apêndice 1, entre outras;
 - iii. Realizar testes às aplicações Web, de acordo com os testes descritos no apêndice 2, entre outros testes que se entendam efetuar;
 - iv. Realizar testes aplicativos exaustivos, referenciados no apêndice 3, testando as funcionalidades de maior risco, entre outras;
 - v. Fornecer reporte de todas as atividades de teste por data e ativos incluídos no âmbito dos testes;
 - vi. Providenciar reporting das Vulnerabilidades Identificadas, à medida que são identificadas, devendo as mesmas ser analisadas e sempre que possível, confirmadas, e não ser resultado de atividades automáticas tais como Scanning. Esta medida visa minimizar a existência de falsos positivos;
 - vii. Classificação das Vulnerabilidades de acordo com a sua severidade:
 - ✓ Baixa
 - ✓ Média
 - ✓ Alta
 - ✓ Muito Alta
 - viii. Providenciar recomendações relativas a todas as vulnerabilidades identificadas, com a indicação de medidas claras que permitam a mitigação das vulnerabilidades em questão;
 - ix. Providenciar apoio às equipas (internas e externas) durante o processo de mitigação das vulnerabilidades, com o objetivo de esclarecer quaisquer questões que visem à adequada mitigação das respetivas vulnerabilidades;
 - x. Realização de follow-up após correção de vulnerabilidades, de forma a confirmar a correta mitigação das vulnerabilidades reportadas. Estas atividades deverão acontecer nos seguintes períodos após a finalização dos testes:
 - ✓ 3 meses – 10 dias de follow-up
 - ✓ 6 meses – 10 dias de follow-up
- d) O Adjudicatário deverá apresentar um modelo proposto de Gestão Operacional do Serviço que assegure a realização de reuniões periódicas de Operacionalização do serviço. Durante as diferentes fases deverá ser garantida a realização de uma reunião de acompanhamento semanal. O objectivo será a análise dos resultados dos testes e sugestões para mitigação das vulnerabilidades;
- e) O Adjudicatário deverá disponibilizar um interlocutor que assegure a Gestão do Serviço e que estabeleça os contactos com o IEFP e garanta a Coordenação Técnica e Operacional do Serviço;
- f) O serviço proposto deverá contemplar um modelo que permita a adaptação do âmbito definido e que permita contemplar a evolução e alterações normais que o IEFP possa efetuar ao seu âmbito durante o curso do serviço. O IEFP poderá assim informar as alterações que pretende introduzir para que sejam objeto de testes.
- g) A resolução/mitigação das vulnerabilidades é da responsabilidade do IEFP e será apoiada pelo adjudicatário;
- h) No âmbito dos serviços a prestar, o IEFP fornecerá os users para a realização dos testes;
- i) O Adjudicatário terá de comunicar ao IEFP, no início dos testes, os IPs que irá utilizar;



- j) Em caso algum os testes poderão ser realizados a partir de IPs diferentes dos comunicados anteriormente. Quando tal tenha de ocorrer devem previamente ser comunicados e aprovados pelo IEFP;
- k) O adjudicatário não poderá realizar, no âmbito do serviço e de forma explícita e premeditada, quaisquer testes de Denial of Service sem prévia autorização do IEFP. Pretende-se evitar situações que levem à interrupção dos sistemas informáticos. Desta forma, o adjudicatário deverá evitar, sempre que possível, a ocorrência destas situações e deve comprometer-se a contactar de imediato o IEFP sempre que alguma situação anómala se verificar de modo a reportar e a normalizar esse serviço.
- l) Comunicar ao IEFP as vulnerabilidades identificadas, à medida que vão sendo descobertas, assim como as respetivas recomendações;
- m) Prestar os esclarecimentos a todas as dúvidas colocadas e acompanhar o IEFP, ou terceiros por si designados, na resolução das vulnerabilidades identificadas;

2. Plataforma para gestão dos serviços prestados

Pretende-se que, como parte integrante do serviço, seja disponibilizada uma Plataforma de Gestão do Serviço, que possibilite o acompanhamento dos testes que compõem o serviço e que possibilite a extração dinâmica de relatórios. A plataforma deverá suportar, entre outras, as seguintes funcionalidades:

- a) Comunicação segura das vulnerabilidades identificadas;
- b) Identificar os tipos de ativos / ativos do IEFP, IP abrangidos no serviço em questão;
- c) Permitir a extração dinâmica de relatórios com base nos parâmetros diversos, tais como: data, tipo de vulnerabilidades, estado, tipo de ativos/ativos e estado da vulnerabilidade;
- d) Suportar multiutilizadores e com a possibilidade de configuração de perfis e permissões por tipo de utilizadores;
- e) Suportar autenticação forte para os utilizadores;
- f) Disponibilizar métricas de risco por tipo de ativo de acordo com o estado das vulnerabilidades reportadas.
- g) Permitir analisar o histórico associado à evolução de cada vulnerabilidade reportada.

Os concorrentes deverão apresentar na resposta a este caderno de encargos uma descrição da plataforma em questão e das funcionalidades apresentadas. Poderá o IEFP IP, solicitar no âmbito deste concurso uma demonstração da plataforma como forma de clarificar algumas questões sobre o funcionamento da mesma.

Cláusula 29.^a

Recursos do adjudicatário

- 1. Independentemente de quaisquer outros que se venham a revelar necessários, o adjudicatário deverá disponibilizar os seguintes recursos técnicos:
 - a) Equipa experiente e multidisciplinar na realização de Testes de Segurança da Informação, que permita a realização dos testes com base em inteligência coletiva;
 - b) Equipa dedicada à prática de Testes de Segurança de Informação com, pelo menos, 5 elementos certificados Offensive Security Certified Professional (OSCP);
- 2. O adjudicatário deverá dispor, pelo menos de certificações ISO 27001 e ISO 9001.
- 3. Os recursos apresentados devem falar e escrever fluentemente em português.



Apêndice 1 – Testes às Vulnerabilidades na Infraestrutura

Categoria	Objetivos
Levantamento da Rede / Enumeração da Rede	• Descobrir dispositivos • Identificar paths das comunicações e facilitar determinação da arquitetura de rede
Portas de Rede e Identificação de Serviços	• Descobrir dispositivos Ativos • Descobrir portas abertas e serviços/aplicações associadas
Análise/Scanning de Vulnerabilidades (inclui rede de servidores das delegações regionais)	• Identificar IPs e portas abertas • Identificar vulnerabilidades conhecidas • Identificar vulnerabilidades desconhecidas • Facultar assessoria na mitigação das vulnerabilidades descobertas • Pentest à infra-estrutura WIFI. • Pentest à VPN.
Password Cracking	• Identificar passwords e políticas de passwords não robustas
Ações de phishing ou outras ações de engenharia social	• Testar quer procedimentos, quer o elemento humano (consciencialização do utilizador)



Apêndice 2 – Testes às Vulnerabilidades nas Aplicações Web

Categoria	Objetivos
Recolha e compilação da informação	• Recolher o máximo de informação possível sobre uma aplicação-alvo
Testes às Configurações de Gestão	• Analisar a infraestrutura e topologia da arquitetura
Testes às Autenticações	• Perceber como funciona o processo de autenticação e usar a informação para subverter o mecanismo de autenticação
Gestão das Sessões	• Segurança da Aplicações
Testes às Autorizações	• Possibilidade de ultrapassar o esquema de autorizações • Encontrar maneiras para escalar privilégios
Testes à lógica do negócio	• Vulnerabilidades relacionadas com o negócio
Testes à Validação de Dados	• Aplicação valida de forma suficiente dados de entrada antes de os utilizar
Testes Denial of Service	• Com foco na camada aplicacional, ataque à disponibilidade que pode ser influenciada por apenas um utilizador malicioso numa única máquina
Testes aos Serviços Web	• Vulnerabilidades nos Serviços Web
Testes AJAX	• Vulnerabilidades Asynchronous JavaScript and X



Apêndice 3 – Testes aplicacionais exaustivos

No mínimo, deverão ser executados os Testes abaixo identificados em função dos tipos de ativos objeto de teste:

- XSS Persistente;
- XSS Refletido;
- Execução de código aplicacional arbitrário remotamente;
- Execução de comandos SQL arbitrários através da aplicação (SQL Injection);
- Execução de pedidos SOAP arbitrários a partir da aplicação (SOAP Injection);
- Execução de queries LDAP arbitrárias através da aplicação (LDAP Injection);
- Path arbitrárias através da aplicação (Ex: PATH Injection);
- Manipulação de valores em Hidden Fields;
- Manipulação de valores em Cookies e headers;
- Manipulação de parâmetros submetidos;
- Bypass de validações de segurança realizadas unicamente do lado do cliente (ex: JavaScript);
- Alteração do fluxo aplicacional em processos multi-etapa;
- Utilização incorrecta de estados/relações de confiança na aplicação;
- Realização de transacções não previstas.