tic.gov.pt

Estratégia Cloud da AP

Modelo de Peças Concursais

Versionamento

Versão	Elaboração	Data
1	Catarina Chiolas (eSPap), Fernando Pereira (IISS), Helena Ramos (MNE), Isabel Gouveia Moura (AT), Jéssica Domingues (CNCS), João Alves (CNCS), José Franco (FCCN), José Miguel Gonçalves (IISS), Maria Celeste Rodrigues (AT), Mário Nogueira (IP), Raul Martins (Portugal Digital), Ruben Silveira (eSPap), Susana Nunes (INCM)	2021-08-02

Índice

1. Introdução

A elaboração das peças concursais para aquisição de serviços *Cloud*, em modelo de serviço IaaS, PaaS ou SaaS - *per si* ou combinadas, apresenta-se atualmente, seja pela novidade, complexidade ou volatilidade, como um desafio para as diferentes entidades da Administração Pública.

Uma das maiores dificuldades do processo de contratação prende-se com a disparidade entre a rigidez imposta pelo CCP aos Adjudicantes e a forma como os CSPs comercializam a sua oferta, muito ágil e orientada a uma metodologia "*pay as you go*".

Neste contexto, foi elaborado o presente documento, não como um modelo *standard*, fechado e acabado, mas como um guião de apoio à identificação de um conjunto de requisitos técnicos, passíveis de serem enquadrados num caderno de encargos, alertando para as dificuldades e obstáculos associados a cada um.

A solução apresentada deverá estar em conformidade, ao longo do período contratualizado para a prestação de serviços, com as diretrizes que vierem a ser definidas pelo CTIC. Para tal, o CSP deverá tomar medidas para se manter informado das políticas e práticas regulamentadas por este organismo, colocando em prática os requisitos de conformidade e interoperabilidade definidos.

Perante a complexidade do processo de contratação, seja ao nível do objeto, seja ao nível das condições contratuais, sugere-se que, a montante, seja efetuada uma consulta preliminar ao mercado, com o objetivo não apenas de refinar os requisitos da solução, como também de os adequar à oferta existente.

1.1. Glossário

Adjudicante	O Organismo Público, o contratante, a entidade adjudicante, o CSC (*Cloud Service Client*)
API	*Application Programming Interface*
CCP	Código de Contratação Pública
CEFR	*Common European Framework of Reference*
CMIS	*Content Management Interoperability Services*
CMMI	*Capability Maturity Model Integration*
CSP	*Cloud Service Provider*, o adjudicatário, o contratado
CTIC	Conselho para as Tecnologias de Informação e Comunicação na Administração Pública
Data Egress	Transferência de dados da infraestrutura do CSP para *on-premises* ou outro CSP; tem o mesmo significado que *Data Outbound*
Data Outbound	Vide *Data Egress*
DL	Decreto-Lei
EUCS	Esquema de Certificação Europeu de Cibersegurança para serviços *Cloud (European Cybersecurity Certification Scheme for Cloud Services)*
IaaS	*Infrastructure as a Service*
ITIL	*Information Technology Infrastructure Library*
LAN	*Local Area Network*
LDAP	*Lightweight Directory Access Protocol*
PaaS	*Platform as a Service*
QNRCS	Quadro Nacional de Referência para a Cibersegurança
RCM	Resolução do Conselho de Ministros

REST	*Representational State Transfer*, um *standard* de *Web Services*
RGPD	Regulamento Geral Proteção de Dados, Lei n.º 58/2019, de 8 de agosto
RNID	Regulamento Nacional de Interoperabilidade Digital, aprovado pela RCM n.º 2/2018, de 5 de janeiro, e pelo DL n.º 83/2018, de 19 de outubro
RPO	*Recovery Point Objective*: após falha catastrófica, que período de tempo não está abrangido por cópia de segurança
RTO	*Recovery Time Objective*: por quanto tempo pode o sistema estar indisponível
SaaS	*Software as a Service*
SAML	*Security Assertion Markup Language*
SOAP	*Simple Object Access Protocol*, um *standard* de *Web Services*
SSO	*Single Sign On*, uma metodologia de autenticação em que a mesmo é efetuada apenas uma vez para, subsequentemente, possibilitar o acesso a múltiplos sistemas
VM	*Virtual Machine*, Máquina Virtual
VPN	*Virtual Private Network*

2. Objeto

O Adjudicante deve enquadrar o procedimento de aquisição de serviços *cloud* num dos modelos de disponibilização – público, privado, comunitário ou híbrido – mas não necessita de fazê-lo relativamente ao modelo de serviço – IaaS, PaaS ou SaaS. Estes modelos estão descritos abaixo.

A aquisição será subordinada a um único modelo de serviço ou a uma qualquer combinação dos mesmos. No entanto, este modelo não é o foco principal do objeto contratual uma vez que, salvo algumas exceções, um determinado serviço a contratar será naturalmente categorizado num dos modelos.

As exceções podem acontecer, por exemplo, devido ao Adjudicante impor requisitos de compatibilidade por forma a manter uma arquitetura o mais similar possível ao que tem na altura, seja ela *on* ou *off-premises*. Nestes casos pode querer adquirir infraestrutura *cloud* com vista à instalação de licenças que pretende adquirir de uma determinada componente (um motor de base dados, por exemplo). Num caso destes, as *guidelines* deste documento aplicar-se-ão única e exclusivamente à componente de infraestrutura *cloud* a adquirir, uma vez que a aquisição das licenças da componente a instalar segue *guidelines* já conhecidas do processo de aquisição tradicional de tecnologias de informação.

Existem três formas de especificar um objeto contratual. Ou este é orientado à necessidade, sendo desta maneira o CSP livre de encontrar possíveis soluções para o mesmo (perante uma determinada necessidade de negócio que pode ser resolvida com a adoção de uma aplicação em modelo SaaS, por exemplo), ou então é orientado à solução, e desta forma são especificadas as componentes que se pretendem adquirir (na migração uma aplicação *on-premises* para a *cloud*, em que o Adjudicante define a totalidade da arquitetura final, por exemplo). Existe ainda um modelo híbrido, em que algumas componentes da arquitetura em *cloud* são especificadas pelo Adjudicante e outras partes da arquitetura não são tão bem conhecidas, sendo, neste caso, necessário que o Adjudicante especifique o que pretende adquirir, em linguagem natural, dando a conhecer os requisitos funcionais e não funcionais que espera serem satisfeitos nestas partes da arquitetura.

Em qualquer dos casos, e sendo que este documento parte integrante da Estratégia Cloud para a Administração Pública em Portugal, deve ser referido que o concorrente deverá responder com soluções baseadas em ofertas *cloud*.

São exemplos de objeto contratual qualquer necessidade funcional e/ou não funcional, como é o caso da aquisição de aplicações, *hosting* ou *housing* de ambientes e acesso a plataformas, ou qualquer especificação de intenção de compra de serviços *cloud* por componente, tais como serviços de computação, *containers*, armazenamento, *backup* e *cold storage*, *networking* e comunicação, segurança e gestão de identidades, motores de bases de dados, plataformas e ferramentas de desenvolvimento, integração aplicacional, acesso a ferramentas de migração, serviços analíticos e inteligência artificial, plataformas de *Big Data*, *blockchain*, serviços de gestão monitorização, *data streaming*, entre muitos outros.

2.1. Modelos de Disponibilização

Os serviços *cloud* são prestados em diferentes modelos de disponibilização.

Na *cloud* pública os recursos são detidos e operados por um CSP externo e disponibilizados através da internet, sendo disponibilizadas soluções padrão para todos os clientes. O acesso à infraestrutura básica (computação, armazenamento, redes, plataformas de desenvolvimento, etc.) é partilhado pelos clientes e fornecido pelo CSP.

Na *cloud* privada, os serviços consistem em recursos utilizados exclusivamente por uma empresa ou organização e, por isso, passíveis de serem personalizados. Os serviços e a infraestrutura podem ser alojados na infraestrutura do CSP – *off-premises* - ou na própria infraestrutura da organização – *on-premises*. Em ambos os casos, os recursos são dedicados exclusivamente à organização.

Na *cloud* comunitária, o modelo tem como objetivo disponibilizar serviços a um conjunto de clientes com caraterísticas e necessidades semelhantes, como sejam, objetivos de negócio, preocupações com segurança ou conformidade com regulamentos específicos. Este modelo baseia-se nas premissas essenciais do modelo de *cloud* privada, mas alargando o alcance a mais do que um cliente. Pode ser disponibilizado *on* e *off-premises*.

A *cloud* híbrida é a combinação de duas ou mais tipologias de *cloud*, quer seja pública ou privada. As componentes de uma *cloud* híbrida tipicamente estão interligadas entre si (por exemplo, uma parte dos serviços implementados em *cloud* pública e outros implementados em *cloud* privada).

2.2. Modelos de Serviço

O modelo IaaS é o alicerce da computação em *cloud*, a camada básica e estrutural que garante o seu funcionamento. Neste modelo todos os recursos físicos que possibilitam ao utilizador o armazenamento e a transmissão de dados são fornecidos: servidores, redes, sistemas operativos e soluções de armazenamento. Os sistemas operativos e aplicações tradicionalmente instalados no terminal do utilizador final são virtualizados. A gestão e controlo da infraestrutura, incluindo compra e instalação de hardware, deixam de fazer parte das responsabilidades do utilizador para passarem a ser assegurados pelo CSP.

O modelo PaaS possibilita ao utilizador a implementação de aplicações – próprias ou adquiridas - na *cloud*, por meio de linguagem de programação, bibliotecas, serviços e ferramentas disponibilizadas pelo fornecedor. Uma plataforma pode ser uma base de dados ou um ambiente completo de desenvolvimento ou testes. Embora o utilizador não faça a gestão nem administre a infraestrutura subjacente, detém o controlo das aplicações instaladas e de parte das configurações dos produtos e do ambiente de alojamento das mesmas.

O modelo SaaS é o nível de abstração mais elevado na cloud. Permite a utilização de software alojado na cloud, eliminando a necessidade de compra, instalação e manutenção local da infraestrutura subjacente, que inclui rede, servidores, sistemas operativos e armazenamento.

2.3. Detalhe do Objeto Contratual

Tal como em qualquer tecnologia, também em *cloud* é necessário fornecer o detalhe para que o CSP seja capaz de escolher a oferta que melhor se adequa às necessidades especificadas. Ou, em alternativa, se o modo de definir o objeto contratual for focado nas componentes dos serviços *cloud* a adquirir, então estas devem ser especificadas pela sua natureza funcional, podendo, inclusivamente, fazer referência a soluções existentes (caso o

âmbito seja um *upgrade* ou uma qualquer aposição a uma solução), desde que o apresente de forma indicativa e permita soluções equivalentes, ficando assim o CSP com o ónus de assegurar eventuais migrações sem disrupção de serviço. Exemplos deste detalhe numa aquisição de uma solução de armazenamento, poderá ser definido pela especificação do tipo de armazenamento, *block storage*, *object storage, cold storage*, *provisioned throughput*, etc.. Quanto maior for o detalhe na especificação, melhor e mais adequada será a resposta aos pedidos de proposta.

2.4. Especificação de Volumetrias

Seja qual for a forma de especificação do objeto contratual – a necessidade, a solução, ou o modelo híbrido – interessa ainda especificar os parâmetros de volumetrias envolvidos na previsão de consumo, uma componente determinante na formação do preço.

Na especificação das volumetrias do objeto é ainda aconselhável que sejam dadas indicações da curva de consumo de cada componente ao longo do período contratual (a expetativa de consumo de *cores*, memória ou *storage*, por exemplo) ou de um determinado período de tempo (um ambiente de formação que poderá ser ligado e desligado a pedido, ou um ambiente de qualidade que apenas está ligado em horário laboral, por exemplo) e, desta forma, dar condições aos CSPs de encontrar oportunidades de redução de custos.

As volumetrias devem ser especificadas de acordo com a natureza do objeto contratual, sendo normalmente combinações de várias métricas.

As formas são variáveis, podendo, inclusivamente, ser encaradas de forma distinta entre CSPs. Apresentam-se de seguida alguns exemplos, sendo esta listagem meramente ilustrativa e não exaustiva:

Métrica de consumo	**Intervalo de Medida**	**Exemplos**
Total de utilizadores	(valor absoluto)	Aquisição de uma aplicação
Total de utilizadores	por unidade de tempo	Gestão de identidades
Qualquer múltiplo de unidade bytes (KiB), (MiB), (GiB), (TiB), etc.	(valor absoluto) ou por unidade de tempo	Armazenamento, fluxo de dados entre regiões ou da *cloud* para o centro de dados *on-premises*, *logs* analisados em ferramentas de gestão
Nodes, *cores*, *clusters*, conectores, *load balancer*, ou outras unidades de capacidade	por unidade de tempo	Computação, serviços de bases de dados, etc.
Total de *requests*, *queries,* mensagens	(valor absoluto) ou por unidade de tempo	Serviço de Integração Aplicacional
Total de interfaces	(valor absoluto)	Interfaces IP em instâncias de computação
Total de métricas calculadas	por unidade de tempo	Métricas calculadas em processos de gestão, alarmes, etc.
Total de objetos consumidos	por unidade de tempo	Vídeo em *streaming*
Total de eventos consumidos	por unidade de tempo	Serviços de proteção e segurança
Número de ambientes, Número de *frontends* Número de *pipelines* CI/CD	(valor absoluto)	Plataforma de Desenvolvimento

Número de caixas	(valor absoluto)	Plataforma de E-mail

2.4.1. Comunicações

Dependendo da arquitetura a implementar, um projeto em *cloud* pode resultar em custos particulares de comunicações entre componentes instaladas em diferentes centros de dados, ou mesmo de *outbound* de dados da *cloud* (vide 13. Estratégia de Saída) para os utilizadores das aplicações. Esta rubrica pode não ser fácil de estimar e é, mais uma vez, dependente da forma de especificação do objeto contratual – a necessidade, a solução, ou o modelo híbrido. A necessidade de ter um controlo particular desta rubrica pode ser relevante para que seja entendido se uma determinada proposta está devidamente dimensionada para responder ou não às necessidades do Adjudicante.

2.5. Agrupamento de Componentes do Objeto Contratual

As diversas componentes da solução deverão ser agregadas por funcionalidade, objetivo, etc., sempre que possível. Desta forma, será possível não só dar melhor visibilidade das peças que se pretendem contratar, como também reutilizar alguns requisitos partilhados pelas componentes inseridas em cada tipo de agrupador, como é o caso da volumetria.

Um exemplo corrente deste tipo de organização é a separação das peças por ambientes: desenvolvimento, integração, qualidade, formação, pré-produção, produção, etc.. Neste exemplo podemos dar condições de volumetria diferentes para cada agrupador e obter propostas mais económicas, uma vez que nem todos os ambientes precisam de estar ativos durante as 24 horas do dia.

2.6. Serviços de Consultoria ou de Execução de Projeto

Estes serviços compreendem todos os serviços prestados por equipas de trabalho, distinguindo-se, desta forma, da oferta tecnológica que em modelo *cloud* também é referida como serviço (em inglês "*as a service*").

Devem ser incluídos neste capítulo todos os serviços disponibilizados pelo CSP com ou sem valorização comercial, incluindo atividades de divulgação, informação, conceção, consultoria, planeamento, desenho, implementação, verificação de qualidade, disponibilização de soluções, suporte, formação, operação, governança, gestão específica ou no sentido lato, entre muitos outros.

Estes serviços não são, na sua natureza, objetivamente diferentes de outros serviços adquiridos fora do contexto *cloud* e, por este motivo, não serão explorados neste documento. Serão diferentes sim, mais uma vez nos detalhes, que muita têm relação têm com as especificidades do objeto contratual enquanto descrição tecnológica. Em qualquer caso, é necessário dar relevo a duas formas muito diferentes de entregar estes serviços por parte dos proponentes. Ou o serviço é entregue em modo de projeto com uma determinada valorização e para o qual o proponente assume a responsabilidade de estruturar uma equipa capaz de executar o projeto a que se propõe, ou então o contratante especifica as necessidades em termos de perfis específicos para o cumprimento de determinados objetivos. Estes perfis são normalmente contratados num modelo que indica o número de horas/dias por recurso contratado. Neste caso aconselha-se a consulta do "Acordo quadro para a prestação de serviços de consultadoria, desenvolvimento e manutenção de software" (eSPap, I.P.), onde estão elencadas especificações de perfis para especialidades técnicas orientadas à *cloud*.

A definição do perfil poderá englobar os seguintes atributos:

- Objeto e descrição do projeto da prestação de serviços;
- Perfil do recurso pretendido (arquiteto, operador *sysops*, etc.);
- Data de início e de término da prestação;
- Requisitos relacionados com senioridade e experiência profissional;
- Requisitos relacionados com certificações profissionais.

3. Arquitetura, Componentes e *Performance*

3.1. Infraestrutura Física

A infraestrutura física afeta à disponibilização do serviço deverá estar alojada em território da União Europeia, oferecendo, pelo menos, duas localizações (regiões) distintas, suficientemente afastadas para oferecerem redundância, podendo o Adjudicante migrar serviços entre as mesmas de forma simplificada, via uma interface *Web* ou comandos de API.

Esta deve estar alojada em centros de processamento de dados de alta disponibilidade, em termos de estabilidade das redes de energia, refrigeração, telecomunicações e segurança do perímetro, de acordo com as normas vigentes.

A capacidade da infraestrutura física deve ser tal que permita adicionar recursos, plataformas, *software* e/ou outros serviços, consoante a modalidade contratada, em modelo de autoaprovisionamento (*self servicing*) com tempos de resposta de acordo com os níveis de serviço.

Deve garantir a criação de uma arquitetura escalável que acompanhe o crescimento do negócio, sem a necessidade de reconfigurar a infraestrutura física.

3.1.1. Serviços sob Procura

O CSP deve garantir que apenas os recursos contratados e necessários ao funcionamento do negócio/infraestrutura são de facto alocados.

3.1.2. Ubiquidade

Os serviços e dados armazenados na *cloud* devem poder ser facilmente acedidos de qualquer lugar com acesso à internet, através de diferentes dispositivos, não apenas de computadores de mesa ou portáteis, mas também de *tablets* ou telemóveis.

3.1.3. Aumento dos Recursos Utilizados

O serviço deve garantir a facilidade de expansão de recursos virtuais ou físicos utilizados, permitindo o redimensionamento da infraestrutura em função das necessidades, de forma fácil e segura.

3.1.4. Elasticidade

O serviço deve garantir a alocação de mais ou menos recursos em função:

- Da quantidade de dados a armazenar;
- Da capacidade de processamento de que os sistemas podem vir a necessitar para funcionarem com a devida *performance*;
- Do número estimado de transações que serão realizadas por período de tempo.

3.2. Orquestração

O serviço deve disponibilizar ferramentas para automatizar os processos de gestão de serviço, com o objetivo de minimizar a realização de tarefas manuais na gestão e otimização dos serviços *cloud*.

Isto visa também otimizar o número de tarefas automáticas para execução de ações operacionais, detetar e responder a falhas ou potenciais falhas e reduzir a necessidade de abertura de pedidos de alteração e suporte por parte do Adjudicante.

3.3. Integração com Serviços de Diretório

O serviço de *cloud* deve ter incluído suporte para integrações com as arquiteturas de Autenticação e Autorização previstas para a Administração Pública portuguesa e suportar as componentes tecnológicas basilares e abertas.

3.4. Comunicações

Deve existir uma camada de acesso LAN para assegurar a interconectividade entre todas as camadas da solução de *cloud* a jusante, permitindo, desta forma, o estabelecimento de sessões lógicas entre os diferentes serviços disponibilizados entre as camadas de IaaS, PaaS e SaaS.

A ligação do CSP à Internet em todas as regiões deve ser redundante e de alta disponibilidade.

Os custos do tráfego, externo ou interno, dos serviços *cloud* devem ser conhecidos à partida e com recurso a regras de cálculo claras e padronizadas.

No caso do tráfego entre regiões, e caso o Adjudicante assim o entenda, pode ser exigido que este esteja isento de custos adicionais. No entanto, deverá ter em conta que nem todos os CSPs suportam esta forma de contratação, optando normalmente por contabilizar este tipo de transferência de forma autónoma.

3.5. Resiliência

Para além das salvaguardas necessárias para cumprir o RPO definido no âmbito dos níveis de serviço, o fornecedor deve garantir a necessária resiliência do sistema de forma a possibilitar a recuperação em caso de avaria ou falha catastrófica, preferivelmente *off site*, eventualmente noutra região.

O sistema deve estar sujeito a um Plano de Continuidade de Negócio, da responsabilidade do CSP, cuja componente de *Disaster Recovery* deve prever, para além dos níveis de serviço, níveis de suporte, capacidade de monitorização e substituições de peças de *hardware* e *software*, a metodologia e frequência dos testes regulares de recuperação.

3.6. IaaS

A solução deve providenciar uma API de controlo em REST, sendo disponibilizada toda a documentação e bibliotecas de acesso em linguagens de programação amplamente usadas.

Deve ter bibliotecas geridas e atualizadas pelo CSP de imagens dos sistemas operativos amplamente usados como Linux e Windows.

Deve ter bibliotecas geridas pelo CSP de serviços de imagens de *appliances* como concentrador VPN, *firewall* ou *load-balancer*.

Deve ainda ter a capacidade de migração de VMs entre *hypervisors* e de criação de *snapshots*.

3.7. PaaS/SaaS

O serviço a disponibilizar deve estar acessível a partir de vários dispositivos pelo Adjudicante através de uma interface simples, tal como um navegador ou uma interface de uma aplicação.

A aplicação/solução deve ser parametrizada preferencialmente pelo Adjudicante, sendo também possível, especialmente em PaaS, que algumas dessas tarefas sejam executadas apenas pelo CSP. Tudo o resto será mantido pelo CSP.

A escalabilidade horizontal deve ser garantida, devendo a solução ter elasticidade e resiliência para suportar os picos de carga sazonais do negócio e qualquer anomalia com impacto na disponibilidade.

O CSP deve garantir a evolução da aplicação / solução / produto, bem como a adaptação a novos requisitos funcionais.

4. Segurança

No âmbito do serviço a contratar deve ser assegurada a confidencialidade de toda a informação tratada no âmbito do objeto contratual e o tratamento de informação classificada de acordo com a RCM n.º 50/88, de 3 de dezembro, que aprova as instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas (SEGNAC 1), bem como a proteção de dados pessoais nos termos da legislação europeia e nacional aplicável.

Os produtos, serviços e/ou processos a adquirir devem refletir e ter em consideração os pressupostos e boas práticas referenciadas no QNRCS, disponibilizado em https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf.

Quando aplicável, a arquitetura de segurança da solução deve cumprir os requisitos técnicos para a proteção de dados pessoais, de acordo com a RCM n.º 41/2018, de 28 de março, disponível em https://data.dre.pt/eli/resolconsmin/41/2018/03/28/p/dre/pt/html, agindo o CSP em conformidade com tais requisitos.

Quando aplicável, a disponibilização de ferramentas tecnológicas deverá respeitar os princípios de segurança e usabilidade comumente associados às boas práticas de desenvolvimento, instalação e configuração, assim como prever a realização de adequados testes de segurança com a metodologia referenciada no OWASP *Web Security Testing Guide*, disponível em https://owasp.org/www-project-web-security-testing-guide/, apresentando, no final, um relatório dos testes efetuados e resultados obtidos.

Adicionalmente aos requisitos supra referenciados, importa referir a existência do EUCS, aplicável a todos os tipos de serviço *cloud*, que tem por objetivo harmonizar a segurança dos serviços cloud com os regulamentos da União Europeia, padrões internacionais, melhores práticas industriais, bem como com as certificações existentes nos Estados-Membros, através de certificados específicos que serão aplicáveis em todos os Estados-Membros.

O Regulamento n.º 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril, estabelece, entre outros, o enquadramento europeu para a certificação da cibersegurança de produtos, serviços e processos de TIC, assim como a criação e definição de esquemas de certificação europeus individualizados e baseados no risco. Assim, os diferentes Estados-Membros podem recorrer à certificação europeia no contexto da adjudicação de contratos públicos e da Diretiva n.º 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro, de forma voluntária, salvo disposição em contrário no direito da União ou dos Estados-Membros.

Ao momento da criação deste documento, o EUCS é disponibilizado apenas numa versão preliminar, com a necessidade de formalização do enquadramento legal, criação de estruturas de certificação e respetivos mecanismos de garantia. Neste sentido, e para conveniência, foram traduzidos e disponibilizados nos anexos I a IV os conjuntos de requisitos de referência de segurança em três níveis de garantia cumulativos (“Básico”, “Substancial” e “Alto”), de forma a serem passíveis de ser utilizados para fins de contratação pública. O teor destes anexos é orientador e não desonera a consulta da versão original do documento, que poderá ser consultada em https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme. Os níveis são os seguintes:

- O Nível de garantia Básico deve ser adequado para serviços *cloud* para dados e sistemas não críticos, conferindo uma garantia limitada de que o serviço *cloud* é

construído e operado com procedimentos e mecanismos para atender aos requisitos de segurança correspondentes a um nível destinado a minimizar os riscos básicos conhecidos de incidentes e ataques de cibersegurança;

- O Nível de garantia Substancial deve ser adequado a serviços, sistemas e dados críticos para o negócio, de modo a fornecer uma garantia razoável de que o serviço *cloud* é construído e operado com procedimentos e mecanismos para minimizar riscos de segurança conhecidos e o risco de incidentes e ataques realizados por atores com habilidades e recursos limitados;
- O Nível de garantia Alto deve ser adequado para serviços *cloud* para atender a requisitos de segurança específicos (excedendo o nível 'substancial') para dados e sistemas críticos para a missão da organização, devendo ser construídos e operados com procedimentos e mecanismos para minimizar o risco de ataques de cibersegurança de última geração e *zero-day* realizados por atores com habilidades e recursos significativos.

De salientar que este esquema reconhece que a responsabilidade dos níveis de segurança está dividida entre o CSP e o Adjudicante, não impondo quaisquer restrições sobre a localização geográfica do tratamento e armazenamento dos dados; no entanto, requer que o CSP seja transparente acerca desta informação e que a disponibilize ao Adjudicante.

5. Perfis

A solução deverá permitir a criação e a configuração de competências dos utilizadores do Adjudicante, via sistema de gestão dos recursos *cloud*, de forma a atribuir competências distintas a utilizadores distintos, como as de administração, utilização, contabilização de consumos e outros perfis de utilizadores a definir.

A gestão dos utilizadores e respetivas permissões deve ser efetuada através de uma interface *Web* ou comando de API.

Deve ser possível agrupar utilizadores em conjuntos dinâmicos e definir permissões para esses mesmos conjuntos.

Deve ainda existir, pelo menos, os perfis de super-administrador e de leitor de registos (*logs*).

5.1. IaaS

Nos sistemas de operação e gestão deve ser possível ao super-administrador configurar quotas máximas de utilização de recursos, por utilizador ou conjunto de utilizadores, possibilitando, assim, que este possa gerir automaticamente os recursos dentro desses limites.

5.2. PaaS

Os gestores das aplicações devem poder utilizar um *backoffice* que lhes permita criar e configurar perfis de utilizador específicos estabelecidos com base em meta dados.

A definição das funções de utilizador deve ser independente de ambiente para ambiente.

Ao nível da plataforma devem existir, pelo menos, os perfis de desenvolvedor e publicador.

6. Integrações

As soluções disponibilizadas ou geradas pela plataforma devem permitir SSO, seja via sistema de autenticação proprietário, seja recorrendo à utilização de *Identity Providers* externos, de onde também receberá *memberships* e/ou *claims*.

Devem, ainda, cumprir os requisitos contemplados no RNID, nomeadamente, mas não só, ao nível dos formatos de documentos estruturados e não estruturados, dos *standards* de interfaces *Web*, e dos protocolos de *streaming* e de correio eletrónico.

6.1. PaaS/SaaS

Devem ser assegurados os mecanismos de Autenticação e Autorização previstos para a Administração Pública portuguesa.

A plataforma deve providenciar uma forma de acesso a repositórios documentais externos.

A plataforma deve ter a capacidade de publicar automaticamente qualquer componente de integração num catálogo partilhado de serviços que pode ser explorada e reutilizada por outras soluções.

A plataforma deve permitir a integração com sistemas externos, nomeadamente ERPs, CRMs, Gestão Documental, BPMs, etc..

A plataforma deve permitir a integração com os principais sistemas gestores de bases de dados relacionais (Oracle, SQL Server, MySQL, etc.) e não relacionais (MongoDB, CouchDB, Azure Cosmos DB, etc.).

7. Normalização e Regras

7.1. Obrigatórias

Devem ser satisfeitas as acreditações exigidas pelo Estado Português.

7.2. Recomendadas

- Certificação de qualidade ISO 9001;
- Certificação de segurança da informação ISO/IEC 27001 para a componente *cloud* proposta; esta certificação poderá ter de ser obrigatória, dependendo do selo de segurança exigido;
- Certificação de segurança da informação ISO/IEC 27017 - *Information technology -- Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud service*;
- Certificação de segurança da informação ISO/IEC 27018 - *Information technology -- Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*;
- Certificação de segurança da informação ISO/IEC-27036-4 - *Information technology -- Security techniques - Information security for supplier relationships -- Part 4: Guidelines for security of cloud services*.

Nota: Neste âmbito salienta-se a existência dos Níveis de Garantia de Segurança que, através do Esquema de Certificação Europeu de Cibersegurança para os serviços *Cloud*, tem como objetivo diminuir a necessidade de especificação dos padrões internacionais, práticas industriais e certificações existentes nos Estados-Membros, sendo a metodologia utilizada pelo EUCS híbrida: baseada tanto na metodologia ISO17021 que é usada para certificações ISO27001 e na metodologia ISAE3402, usada por muitas empresas para obter relatórios de garantia sobre a segurança de seus sistemas de informação.

7.3. Facultativas

- Satisfação das orientações do programa "*Data Centres Energy Efficiency EU Code of Conduct*", disponível em https://e3p.jrc.ec.europa.eu/communities/data-centres-code-conduct;
- Certificações ambientais:
  - ISO 14001 - *Environmental Management*;
  - ISO 50001 - *Energy management* para gestão de energia;
  - ISO 26000 - *Social Responsibility*.
- Certificação ISO 20000 - Service Management;
- Certificação CMMI.

7.4. PaaS/SaaS

As soluções geradas pela plataforma devem basear-se em normas abertas ou amplamente suportadas pelo mercado e que não envolvam custos específicos de licenciamento por parte dos utilizadores, devendo cumprir o teor do estipulado pela Lei n.º 36/2011, de 21 de junho, e pelo RNID relativamente à obrigatoriedade de utilização de normas abertas.

As componentes *web* devem ser baseadas em *standards* de indústria (HTML5, CSS3, *React*, p. ex.), serem executadas nos *browsers* (Google Chrome, Apple Safari, Microsoft Edge e Mozilla Firefox) e sistemas operativos (Microsoft Windows, Apple macOS e GNU/Linux) com maior quota de mercado; deverão ainda estar conforme os critérios de acessibilidade estabelecidos pelo DL n.º 83/2018, de 19 de outubro.

As interligações com *Identity Providers* externos devem ser efetuadas com recurso a *standards* de mercado, como por exemplo SAML, LDAP, OpenID ou OAuth, sempre sobre canais seguros.

A metodologia de acesso a repositórios externos documentais deve estar de acordo com *standards* de mercado, como por exemplo CMIS.

Os serviços *Web* devem ser consumidos e implementados com recurso tanto a SOAP como a REST.

Quando aplicável, deve ser exigida a compatibilidade das APIs disponibilizadas com pelo menos uma das seguintes normas *de facto*:

- *Compute*:
  - Amazon Elastic Compute Cloud (EC2)
  - OCCI
  - Microsoft Azure API
  - DBCE
  - Google GCE
  - HNX SlipStream
  - OpenStack Nova
- *Storage*:
  - Amazon S3
  - Amazon EBS
  - Microsoft Azure API
  - Ceph RADOSGW
  - CDMI
  - Google Cloud Storage (GCS)
  - OpenStack Swift
  - OpenStack
  - Cinder

8. Níveis de Serviço

Exemplos de níveis de serviço mínimos:

	IaaS	**PaaS**	**SaaS**
Indisponibilidade do serviço (evento anual) – RTO	30 minutos	60 minutos	120 minutos
Tempo mínimo de disponibilidade mensal (base 24x7) = (N.º máximo de minutos disponibilidade - Indisponibilidade) / (N.º máximo de minutos disponibilidade x 100)	99,9%		
Resposta a degradação de serviço	< 30 minutos	< 1 hora	
Primeira resposta não automática ao atendimento telefónico (média mensal)	< 2 minutos		
Primeira resposta não automática a correio eletrónico / Portal *Web* em horário regular (média mensal)	< 4 horas		
Primeira resposta não automática a correio eletrónico / Portal *Web* em horário estendido (média mensal)	< 12 horas		
Autoaprovisionamento de serviços e recursos	Automático		
Resposta do autoaprovisionamento de serviços e recursos	< 10 minutos	< 5 minutos	
Apoio presencial para ligação do Adjudicante à *Cloud* (arranque do serviço)	NBD		
Ações de manutenção programada	00:00 às 06:00 (UTC +1)		
RPO	< 1 hora		
Latência em *Cloud* Pública	< 40 milissegundos		
Latência em *Cloud* Privada	< 30 milissegundos		

9. Penalidades

Quando não sejam cumpridos pelo CSP os níveis de serviço a que está obrigado, por via dos requisitos de serviço definidos no Caderno de Encargos, e desde que tal não resulte de motivos de força maior e sem prejuízo das situações de rescisão contratual previstas, o Adjudicante poderá aplicar penalidades pecuniárias, calculadas de acordo com o tipo de incumprimento observado, de montante a fixar em função da gravidade do incumprimento, com um mínimo correspondente a, por exemplo, 1% do preço contratual por cada dia de atraso.

Em caso de resolução contratual por incumprimento do CSP, o Adjudicante poderá exigir-lhe uma pena pecuniária até 20% do preço contratual.

Relativamente aos níveis de serviços anteriormente referidos, poder-se-ão aplicar exemplificativamente as seguintes penalidades:

	Penalidade
Tempo mínimo de disponibilidade mensal (base 24x7)	Até x % do preço contratual mensal por cada centésima percentual abaixo do nível de serviço contratado
Primeira resposta não automática ao atendimento telefónico (média mensal)	Até x % do preço contratual mensal por cada minuto de atraso
Primeira resposta não automática a correio eletrónico / Portal *Web* em horário regular (média mensal)	Até x % do preço contratual mensal por cada hora de atraso
Primeira resposta não automática a correio eletrónico / Portal *Web* em horário estendido (média mensal)	Até x % do preço contratual mensal por cada hora de atraso
Autoaprovisionamento de serviços e recursos	Até x % do preço contratual mensal pelo incumprimento
Resposta do autoaprovisionamento de serviços e recursos	Até x % do preço contratual mensal por cada minuto de atraso
Apoio presencial para ligação do Adjudicante à *Cloud* (arranque do serviço)	Até x % do preço contratual mensal por cada dia completo de atraso
Ações de manutenção programada	Até x % do preço contratual mensal por cada hora fora do período temporal acordado

O Adjudicante, independentemente das demais sanções e penalidades previstas na lei e no Contrato, poderá decidir a resolução do contrato quando não sejam cumpridas pelo CSP quaisquer cláusulas contratuais e desde que tal não resulte de motivos de força maior, nomeadamente:

- Quando a solução não corresponder às características estabelecidas;
- Incumprimento definitivo do contrato;
- Incumprimento de ordens, diretivas ou instruções transmitidas no exercício do poder de direção sobre matéria relativa à execução das prestações contratuais;
- Se o valor acumulado das sanções contratuais com natureza pecuniária exceder 20% do preço contratual;
- Nas situações previstas nas alíneas c), d), f) e h) do número 1 do artigo 333.º do CCP.

A resolução do contrato não afetará a parte já cumprida do mesmo se, do ponto de vista do Adjudicante, a tal parte já cumprida tiver interesse para esta entidade, pois, caso contrário, a eficácia será retroativa.

A resolução do contrato não invalida o direito a qualquer ação que venha a ser interposta por parte do Adjudicante, com vista à justa indemnização por perdas e danos eventualmente sofridos.

10. Apoio e Suporte

O CSP deve proporcionar suporte técnico remoto, preferencialmente em língua Portuguesa, de acordo com os tempos de resposta contratualizados disponibilizados em modelo multicanal. Os canais a suportar pelo CSP poderão ser: *email; ticket web;* plataforma de *self-service* ou telefone.

Caso não disponha de pessoal para resposta em língua Portuguesa, então deve poder responder em língua inglesa, pelo menos no nível "B2" como especificado na CEFR.

Devem ser definidos procedimentos de acesso ao suporte técnico em horário regular e estendido, bem como para escalar assuntos:

- Horário regular: de segunda a sexta entre as 8:00 horas e às 20:00 horas (UTC +1);
- Horário estendido: todos os restantes intervalos temporais numa base 24x7 que não se afiguram como horário regular.

Deve ser disponibilizada documentação de apoio à utilização da solução, pelo menos em língua Inglesa.

Devem existir mecanismos de formação de pessoal técnico do Adjudicante em modelo presencial ou *e-learning*.

O modelo de serviços deverá ser suportado por uma ferramenta de gestão de incidentes com disponibilização, alinhada com as práticas ITIL, de *dashboards* que mostram em tempo real os indicadores, consumos e níveis de serviço.

11. Proteção de Dados Pessoais

O CSP tem de cumprir com o que está estabelecido no RGPD, e estar conforme a RCM n.º 41/2018, de 28 de março, com as alterações que lhes vierem a suceder. Deve também cumprir, no aplicável, os requisitos de cibersegurança estabelecidos pela Autoridade Nacional de Cibersegurança, vigentes para projetos SAMA e publicados em https://www.cncs.gov.pt/content/files/SAMA2020_RASRSI_CNCS.pdf.

Os serviços fornecidos devem cumprir as orientações técnicas estabelecidas para a arquitetura de segurança das redes e sistemas de informação para a Administração Pública pela RCM n.º 41/2018, de 28 de março, bem como cumprir os requisitos contemplados no regulamento nacional de interoperabilidade digital publicado na RCM n.º 2/2018, de 5 de janeiro.

O CSP deve comprovar que assegurará que qualquer funcionário, agente ou contratado seu que possa ter acesso aos dados pessoais tratados, esteja sujeito a compromissos de confidencialidade ou obrigações profissionais ou estatutárias de confidencialidade., durante e após a vigência do contrato (Confidencialidade).

O CSP deve comprovar que aplica as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados e contra qualquer outra forma de tratamento ilícito (Segurança). Essas medidas devem compreender pelo menos as seguintes:

- A pseudonimização e a cifragem dos dados pessoais;
- A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de Tratamento;
- A capacidade de detetar uma violação de Dados Pessoais, resolvê-la e relatá-la;
- A capacidade de restabelecer a disponibilidade e o acesso aos Dados Pessoais de forma atempada no caso de um incidente físico ou técnico;
- Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do Tratamento.

O CSP deve assegurar que utilizará os dados pessoais a que tenha acesso única e exclusivamente para efeitos do fornecimento objeto deste contrato (Finalidades dos tratamentos).

O CSP deve comprovar que tem implementados procedimentos para manter registos sobre todas as categorias de tratamento de dados pessoais e atividades realizadas no âmbito do fornecimento do serviço (Registo das atividades de tratamento).

O CSP deve comprovar que tem implementados procedimentos que possibilitem ao adjudicante a satisfação dos pedidos de exercício dos direitos dos titulares dos dados. Estes incluem os direitos de acesso, retificação, apagamento, portabilidade dos dados, limitação do tratamento, de não ficar sujeito a decisões individuais automatizadas e oposição. (Direitos dos titulares dos dados).

O CSP deve comprovar que tem implementados procedimentos que possibilitem a notificação ao adjudicante, por escrito e com a maior brevidade possível qualquer violação de segurança que potencialmente comprometa a segurança de dados pessoais (Notificação de violação de dados pessoais).

O CSP deve comprovar que apenas procederá à transferência de dados para países fora da EU ou organizações internacionais com o consentimento prévio do adjudicante e de acordo com as decisões de adequabilidade da autoridade de controle e dos requisitos expressos no RGPD. Para este efeito, entende-se como transferência internacional de dados, não apenas o movimento destes, mas também o seu acesso através das fronteiras da União Europeia (Transferências internacionais).

O CSP deve poder comprovar que estão implementados procedimentos que, logo que o contrato termine, procederá ao apagamento dos dados pessoais que tiver em seu poder ou devolvê-los-á ao adjudicante, conforme este decidir, e apagará todas as cópias que tiver em seu poder (Cessação do Tratamento).

O CSP obriga-se a garantir que as empresas por ele subcontratadas cumprirão o disposto no RGPD e na demais legislação aplicável, devendo tal obrigação constar dos contratos escritos a celebrar com as entidades por si subcontratadas (Subcontratação).

O CSP deve apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma a que o tratamento de dados satisfaça os requisitos do RGPD, e assegure a defesa dos direitos do titular dos dados, nomeadamente, através da existência e do cumprimento de um código de conduta ou de procedimento de certificação aprovado conforme referido nos artigos 40.° e 42.° do RGPD.

12. Auditabilidade

O sistema deve possibilitar o rastreamento e mapeamento das atividades executadas sobre o mesmo, gerando para isso todos os registos necessários acerca de quem fez o quê, e quando.

O sistema deve fornecer uma consola, de acesso limitado, que permita a consulta destes registos.

Deve ainda ser dada particular atenção aos registos exigidos pelo RGPD, em todas as suas vertentes, estabelecidos em legislação específica.

13. Estratégia de Saída

São várias as eventuais motivações para abandonar ou migrar de um serviço *cloud*, desde os custos da solução até uma alteração de política organizacional, ou mesmo devido a quebra contratual. Para tal processo é necessário evitar o *vendor lock-in*, situação que pode ser descrita como a dificuldade ou incapacidade de abandonar a solução *cloud* contratada.

A estratégia de saída é um plano desenvolvido ainda antes da fase de contratação para garantir que os serviços *cloud* que suportam as atividades de negócio possam ser substituídos ou replicados de forma eficiente e sem interrupções significativas para a empresa.

Pode ser baseado em várias estratégias, sendo que se podem relevar duas, de cloud para *on-premises* e de *cloud* para *cloud*, sendo que para esta última a adoção de um modelo *multi-cloud* desde o início facilitará o processo.

Esta estratégia deve ser tida em conta nas fases de orçamentação e cabimentação, assim como nas fases de definição dos elementos para consulta e dos próprios critérios de adjudicação em termos do custo total do processo, desde eventuais serviços de consultoria até ao *data egress*, custo efetivo e normalmente avultado – crash da infraestrutura *on-premises* com necessidade de reposição total de dados a partir da cloud, mudança/alteração de CSP, por exemplo – mas muitas vezes negligenciado até à altura da saída efetiva.

13.1. *Phase-Out* e Transferência de Conhecimento

O CSP deve indicar o método que se propõe adotar para transferência de know-how para as equipas a designar pelo Adjudicante.

A transferência de know-how inclui todos os manuais técnicos dos equipamentos e formas de acesso remoto aos mesmos, as configurações atuais existentes, o registo de incidentes e de *backlogs* e o inventário atualizado.

Toda a documentação de suporte deverá ser fornecida em suporte digital, incluindo os manuais de instalação, configuração e operação.

A transferência de conhecimento deve ser proposta ao Adjudicante no prazo de 60 dias a contar do início da prestação do serviço e ser executado até 15 dias antes do termo dos efeitos do contrato ou, em caso de extinção do contrato por quaisquer outros motivos, no prazo máximo de 15 dias a contar da respetiva decisão.

Toda a informação deve ser fornecida em formatos neutros e padronizados que possibilitem a sua portabilidade.

Os dados do Adjudicante devem permanecer acessíveis para qualquer função de migração durante pelo menos 90 dias após término da prestação do serviço, período este passível de ser ajustado mediante tipologia do serviço.

Os dados do Adjudicante devem ser eliminados dos serviços do CSP, após o prazo referido no ponto anterior. Deverão ser geradas evidências desta ação no prazo máximo de 15 dias após a eliminação.

13.2. PaaS/SaaS

Caso o Adjudicante assim o entenda, poderá exigir que a plataforma ou serviço a contratar seja passível de ser instalada e executada noutro serviço *cloud* ou, eventualmente, *on-premises*.

14. Monitorização

O sistema deve providenciar um sistema de monitorização que permita ao Adjudicante controlar o inventário de todos os recursos consumidos, assim como a faturação correspondente, tanto em tempo real como para efeitos de histórico.

14.1. IaaS

O serviço a disponibilizar deve fornecer uma lista e resumo dos serviços IaaS disponibilizados, incluindo, mas não restrito a, servidores virtuais, blocos de disco virtuais e recursos de rede.

14.2. PaaS

A plataforma deve assegurar a criação automática de registos de erros, de alertas, de auditorias e de desempenho, seja ao nível da plataforma propriamente dita, seja ao nível de cada solução.

As métricas devem ser capturadas assincronamente para que a *performance* não seja comprometida, sendo posteriormente depositadas em base de dados.

Esses eventos devem ser consultáveis através de consola centralizada própria para o efeito. Deve ainda disponibilizar um painel de controlo de *performance* que facilite a identificação de problemas de desempenho. Esse painel de controle deve utilizar a base de dados de acima mencionada e correlacionar informação - como, por exemplo, quais são as instruções dadas à base de dados que estão a afetar o desempenho de uma certa ação.

O painel de controle também deve destacar automaticamente problemas como a existência de ações ou extensões cujo desempenho esteja abaixo do desejável.

Cada atividade produzida pela equipa de desenvolvimento, gestores de aplicações e administradores de sistemas deve ser registadas. Estes eventos incluem, pelo menos:

- Publicação de novas versões de aplicações ou componentes;
- Remoção de aplicações ou componentes;
- Alterações às configurações da plataforma e soluções;
- Registo de autenticações no sistema;
- Processos de execução em lote;
- Consulta e escrita de dados pessoais.

A plataforma deve disponibilizar métricas de execução, nomeadamente:

- Tempos de execução do servidor;
- Indicação de consumo de tempo no processamento da lógica de negócio ou na integração entre componentes da aplicação;
- Desempenho da rede de comunicações (segregando o tempo médio de execução por operador de rede e o uso da rede Wi-Fi);
- Desempenho do lado cliente (segregando o tempo médio de execução pelo sistema operacional móvel e/ou navegador *web*).

Deve ser disponibilizada informação de contabilização da utilização e faturação em tempo real e permitir a configuração de alertas, por objetivo ou por proximidade ao mesmo, de forma percentual ou absoluta, e reportes sobre consumos dos serviços, incluindo utilizadores.

Deve ser disponibilizado um sistema de previsão de custos de consumo dos serviços contratados mediante necessidades evolutivas do Adjudicante.

O sistema deve também ter a capacidade de monitorização da infraestrutura e geração automática de alertas para intervenções preventivas no sistema e capacidade de geração automática de relatórios de incidentes.

Deve ainda disponibilizar ferramentas de aconselhamento, com base na predição, para a otimização dos recursos dos serviços usados.

15. Critérios de Adjudicação

Salvaguardando-se os princípios da transparência e da concorrência, a adjudicação pressupõe a análise e ordenação das propostas que tenham sido aceites através da aplicação do critério de adjudicação definido nas peças. O critério de adjudicação corresponde ao método de avaliação das diversas propostas apresentadas pelos concorrentes num procedimento de contratação pública, de forma a possibilitar, ao Adjudicante, a escolha da melhor proposta.

Presentemente, e de acordo com o artigo 74.º do CCP, a entidade adjudicante pode adotar um de dois modelos de adjudicação:

- Monofator (designadamente o preço), tendo apenas como limite o preço base estabelecido e desde que as peças do procedimento definam todos os elementos da execução do contrato a celebrar – ou
- Multifator (pela melhor relação qualidade/preço), na qual o critério de adjudicação é composto por um conjunto de fatores, e eventuais subfatores.

Na segunda opção referida podem ponderar-se diversos aspetos da execução do contrato a celebrar, enunciando-se de seguida alguns a título exemplificativo:

- Custos relativos à extração dos dados/sistemas e aplicações:
  - Custo da saída;
- Condições de disponibilização dos serviços;
- Serviços adicionais:
  - Custos com serviços de consultoria;
- Prazos de entrega;
- Critérios de sustentabilidade:
  - Percentagem de *green energy* usada;
- Percentagem de desconto:
  - Percentagem de desconto local;
- Critério de marketing de adoção e suporte:
  - Número de ações de formação, workshops, etc.;
  - Existência de serviço de apoio e suporte local.
- Cumprimento de regras/normas indicadas como facultativas.

16. Anexo I - Categorias de Requisitos de Segurança

Ref.1	Ref.2	Descrição
OIS	**A.1**	**ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO**
OIS	OIS-01	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO
OIS	OIS-02	SEGREGAÇÃO DE FUNÇÕES
OIS	OIS-03	CONTACTO COM AUTORIDADES E GRUPOS DE INTERESSE
OIS	OIS-04	SEGURANÇA DA INFORMAÇÃO NA GESTÃO DE PROJETO
ISP	**A.2**	**POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO**
ISP	ISP-01	POLÍTICA GLOBAL DE SEGURANÇA DA INFORMAÇÃO
ISP	ISP-02	POLÍTICAS E PROCEDIMENTOS DE SEGURANÇA
ISP	ISP-03	EXCEÇÕES
RM	**A.3**	**GESTÃO DE RISCO**
RM	RM-01	POLÍTICA DE GESTÃO DE RISCO
RM	RM-02	IMPLEMENTAÇÃO DE AVALIAÇÃO DE RISCOS
RM	RM-03	IMPLEMENTAÇÃO DE TRATAMENTO DE RISCOS
HR	**A.4**	**RECURSOS HUMANOS**
HR	HR-01	POLÍTICAS DE RECURSOS HUMANOS
HR	HR-02	VERIFICAÇÃO DA QUALIFICAÇÃO E CONFIANÇA
HR	HR-03	TERMOS E CONDIÇÕES DE FUNCIONÁRIOS
HR	HR-04	SENSIBILIZAÇÃO E TREINO DE SEGURANÇA
HR	HR-05	RESCISÃO OU MUDANÇA DE EMPREGO
HR	HR-06	ACORDOS DE CONFIDENCIALIDADE
AM	**A.5**	**GESTÃO DE ATIVOS**
AM	AM-01	INVENTÁRIO DE ATIVOS
AM	AM-02	POLÍTICA DE USO ACEITÁVEL E MANUSEAMENTO SEGURO DE ATIVOS
AM	AM-03	COMISSIONAMENTO E DESCOMISSIONAMENTO DE HARDWARE
AM	AM-04	USO ACEITÁVEL, MANUSEAMENTO SEGURO E DEVOLUÇÃO DE ATIVOS
AM	AM-05	CLASSIFICAÇÃO E IDENTIFICAÇÃO DE ATIVOS
PS	**A.6**	**SEGURANÇA FÍSICA**
PS	PS-01	PERÍMETROS DE SEGURANÇA FÍSICA
PS	PS-02	CONTROLO DE ACESSOS AO LOCAL FÍSICO
PS	PS-03	TRABALHAR EM ÁREAS NÃO PÚBLICAS
PS	PS-04	PROTEÇÃO DE EQUIPAMENTO
PS	PS-05	PROTEÇÃO CONTRA AMEAÇAS EXTERNAS E AMBIENTAIS
OPS	**A.7**	**SEGURANÇA OPERACIONAL**
OPS	OPS-01	GESTÃO DE CAPACIDADE - PLANEAMENTO
OPS	OPS-02	GESTÃO DE CAPACIDADE - MONITORIZAÇÃO
OPS	OPS-03	GESTÃO DE CAPACIDADE - CONTROLO DE RECURSOS
OPS	OPS-04	PROTEÇÃO CONTRA MALWARE - POLÍTICAS
OPS	OPS-05	PROTEÇÃO CONTRA MALWARE - IMPLEMENTAÇÃO
OPS	OPS-06	BACKUP E RECUPERAÇÃO DE DADOS - POLÍTICAS
OPS	OPS-07	BACKUP E RECUPERAÇÃO DE DADOS - MONITORIZAÇÃO
OPS	OPS-08	BACKUP E RECUPERAÇÃO DE DADOS - TESTES REGULAR
OPS	OPS-09	BACKUP E RECUPERAÇÃO DE DADOS - ARMAZENAMENTO
OPS	OPS-10	REGISTO (LOGGING) E MONITORIZAÇÃO - POLÍTICAS
OPS	OPS-11	REGISTO (LOGGING) E MONITORIZAÇÃO - GESTÃO DE DADOS DERIVADOS
OPS	OPS-12	REGISTO (LOGGING) E MONITORIZAÇÃO - IDENTIFICAÇÃO DE EVENTOS
OPS	OPS-13	REGISTO (LOGGING) E MONITORIZAÇÃO - ACESSO, ARMAZENAMENTO E ELIMINAÇÃO
OPS	OPS-14	REGISTO (LOGGING) E MONITORIZAÇÃO - ATRIBUIÇÃO
OPS	OPS-15	REGISTO (LOGGING) E MONITORIZAÇÃO - CONFIGURAÇÃO
OPS	OPS-16	REGISTO (LOGGING) E MONITORIZAÇÃO - DISPONIBILIDADE
OPS	OPS-17	GESTÃO DE VULNERABILIDADES, MAU FUNCIONAMENTO E ERROS - POLÍTICAS
OPS	OPS-18	GESTÃO DE VULNERABILIDADES, MAU FUNCIONAMENTO E ERROS - REGISTO ONLINE
OPS	OPS-19	GESTÃO DE VULNERABILIDADES, MAU FUNCIONAMENTO E ERROS - IDENTIFICAÇÃO DE VULNERABILIDADES
OPS	OPS-20	GESTÃO DE VULNERABILIDADES, MAU FUNCIONAMENTO E ERROS - MEDIÇÕES, ANÁLISES E AVALIAÇÕES DE PROCEDIMENTOS
OPS	OPS-21	GESTÃO DE VULNERABILIDADES, MAU FUNCIONAMENTO E ERROS - ROBUSTECIMENTO DE SISTEMAS
OPS	OPS-22	SEPARAÇÃO DE CONJUNTOS DE DADOS NA INFRAESTRUTURA CLOUD
IAM	**A.8**	**IDENTIDADE, AUTENTICAÇÃO E GESTÃO DE CONTROLO DE ACESSOS**
IAM	IAM-01	POLÍTICAS PARA CONTROLO DE ACESSOS À INFORMAÇÃO
IAM	IAM-02	GESTÃO DE CONTAS DE UTILIZADOR
IAM	IAM-03	BLOQUEIO, DESBLOQUEIO E REVOGAÇÃO DE CONTAS DE UTILIZADOR
IAM	IAM-04	GESTÃO DE DIREITOS DE ACESSO
IAM	IAM-05	REVISÃO REGULAR DOS DIREITOS DE ACESSO
IAM	IAM-06	DIREITOS DE ACESSO PRIVILEGIADO

IAM	IAM-07	MECANISMOS DE AUTENTICAÇÃO
IAM	IAM-08	PROTEÇÃO E ROBUSTEZ DE CREDENCIAIS
IAM	IAM-09	RESTRIÇÕES GERAIS DE ACESSO
CKM	**A.9**	**CRIPTOGRAFIA E GESTÃO DE CHAVES**
CKM	CKM-01	POLÍTICAS PARA USO DE MECANISMOS DE CRIPTOGRAFIA E GESTÃO DE CHAVES
CKM	CKM-02	ENCRIPTAÇÃO DE DADOS EM TRÂNSITO
CKM	CKM-03	ENCRIPTAÇÃO DE DADOS EM REPOUSO
CKM	CKM-04	GESTÃO SEGURA DE CHAVES
CS	**A.10**	**SEGURANÇA DE COMUNICAÇÕES**
CS	CS-01	SALVAGUARDAS TÉCNICAS
CS	CS-02	REQUISITOS DE SEGURANÇA PARA CONEXÃO À REDE DO CSP
CS	CS-03	MONITORIZAÇÃO DE CONEXÕES DENTRO DA REDE DO CSP
CS	CS-04	ACESSO A MÚLTIPLAS REDES
CS	CS-05	REDES PARA ADMINISTRAÇÃO
CS	CS-06	SEGREGAÇÃO DE TRÁFEGO EM AMBIENTES DE REDE PARTILHADA
CS	CS-07	DOCUMENTAÇÃO DE TOPOLOGIA DE REDE
CS	CS-08	REDE DEFINIDA POR SOFTWARE
CS	CS-09	POLÍTICAS DE TRANSFERÊNCIA DE DADOS
PI	**A.11**	**PORTABILIDADE E INTEROPERABILIDADE**
PI	PI-01	DOCUMENTAÇÃO E SEGURANÇA DAS INTERFACES DE ENTRADA E SAÍDA
PI	PI-02	ACORDOS CONTRATUAIS DE FORNECIMENTO DE DADOS
PI	PI-03	ELIMINAÇÃO SEGURA DE DADOS
CCM	**A.12**	**GESTÃO DE ALTERAÇÕES E CONFIGURAÇÕES**
CCM	CCM-01	POLÍTICAS DE ALTERAÇÕES PARA SISTEMAS DE INFORMAÇÃO
CCM	CCM-02	AVALIAÇÃO DE RISCO, CATEGORIZAÇÃO E PRIORIZAÇÃO DE ALTERAÇÕES
CCM	CCM-03	TESTE DE ALTERAÇÕES
CCM	CCM-04	APROVAÇÕES PARA PROVISÃO EM AMBIENTE DE PRODUÇÃO
CCM	CCM-05	REALIZAÇÃO E REGISTO DE ALTERAÇÕES (LOGGING)
CCM	CCM-06	CONTROLO DE VERSÕES
DEV	**A.13**	**DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO**
DEV	DEV-01	POLÍTICAS DE DESENVOLVIMENTO E APROVISIONAMENTO DE SISTEMAS DE INFORMAÇÃO
DEV	DEV-02	SEGURANÇA DA CADEIA DE FORNECIMENTO DE DESENVOLVIMENTO
DEV	DEV-03	AMBIENTE DE DESENVOLVIMENTO SEGURO
DEV	DEV-04	SEPARAÇÃO DE AMBIENTES
DEV	DEV-05	DESENVOLVIMENTO DE FUNCIONALIDADES DE SEGURANÇA
DEV	DEV-06	IDENTIFICAÇÃO DE VULNERABILIDADES DO SERVIÇO CLOUD
DEV	DEV-07	SUBCONTRATUALIZAÇÃO DO DESENVOLVIMENTO
PM	**A.14**	**GESTÃO DE AQUISIÇÕES**
PM	PM-01	POLÍTICAS E PROCEDIMENTOS PARA CONTROLO E MONITORIZAÇÃO DE TERCEIROS
PM	PM-02	AVALIAÇÃO DE RISCO DE FORNECEDORES
PM	PM-03	DIRETÓRIO DE FORNECEDORES
PM	PM-04	MONITORIZAÇÃO DE CONFORMIDADE COM OS REQUISITOS
PM	PM-05	ESTRATÉGIA DE SAÍDA
IM	**A.15**	**GESTÃO DE INCIDENTES**
IM	IM-01	POLÍTICA PARA GESTÃO DE INCIDENTES DE SEGURANÇA
IM	IM-02	TRATAMENTO DE INCIDENTES DE SEGURANÇA
IM	IM-03	DOCUMENTAÇÃO E RELATÓRIOS DE INCIDENTES DE SEGURANÇA
IM	IM-04	DEVER DO USUÁRIO DE RELATAR INCIDENTES DE SEGURANÇA
IM	IM-05	ENVOLVIMENTO DE CLIENTES CLOUD EM CASO DE INCIDENTES
IM	IM-06	PROCESSO DE AVALIAÇÃO E APRENDIZAGEM
IM	IM-07	PRESERVAÇÃO DE EVIDÊNCIAS DE INCIDENTES
BC	**A.16**	**CONTINUIDADE DE NEGÓCIO**
BC	BC-01	POLÍTICAS DE CONTINUIDADE DE NEGÓCIO E RESPONSABILIDADE DA GESTÃO DE TOPO
BC	BC-02	PROCEDIMENTOS DE ANÁLISE DE IMPACTO DE NEGÓCIO
BC	BC-03	PLANEAMENTO DE CONTINUIDADE DE NEGÓCIO E CONTINGÊNCIA
BC	BC-04	TESTES E EXERCÍCIOS DE CONTINUIDADE DE NEGÓCIO
CO	**A.18**	**CONFORMIDADE**
CO	CO-01	IDENTIFICAÇÃO DOS REQUISITOS DE CONFORMIDADE APLICÁVEIS
CO	CO-02	POLÍTICA PARA PLANEAMENTO E REALIZAÇÃO DE AUDITORIAS
CO	CO-03	AUDITORIAS INTERNAS AO SISTEMA DE CONTROLO INTERNO
CO	CO-04	INFORMAÇÕES SOBRE AVALIAÇÃO DO SISTEMA DE CONTROLO INTERNO
DOC	**A.19**	**DOCUMENTAÇÃO DO UTILIZADOR**
DOC	DOC-01	DIRETRIZES E RECOMENDAÇÕES PARA CLIENTES CLOUD
DOC	DOC-02	REGISTO ONLINE DE VULNERABILIDADES CONHECIDAS
DOC	DOC-03	LOCALIZAÇÃO DE TRATAMENTO E ARMAZENAMENTO DE DADOS
DOC	DOC-04	JUSTIFICAÇÃO DO NÍVEL DE GARANTIA PRETENDIDO
DOC	DOC-05	DIRETRIZES E RECOMENDAÇÕES PARA COMPOSIÇÃO

DOC	DOC-06	CONTRIBUIÇÃO PARA O CUMPRIMENTO DOS REQUISITOS DE COMPOSIÇÃO
INQ	**A.19**	**TRATAMENTO DE PEDIDOS DE INVESTIGAÇÃO DE AGÊNCIAS GOVERNAMENTAIS**
INQ	INQ-01	AVALIAÇÃO LEGAL DE INQUÉRITOS DE INVESTIGAÇÃO
INQ	INQ-02	INFORMAR OS CLIENTES CLOUD SOBRE OS PEDIDOS DE INVESTIGAÇÃO
INQ	INQ-03	CONDIÇÕES DE ACESSO OU DIVULGAÇÃO DE DADOS EM PEDIDOS DE INVESTIGAÇÃO
PSS	**A.20**	**SEGURANÇA E SEGURANÇA DO PRODUTO (PSS)**
PSS	PSS-01	TRATAMENTO DE ERROS E MECANISMOS DE REGISTO (LOGS)
PSS	PSS-02	GESTÃO DE SESSÕES
PSS	PSS-03	SOFTWARE DEFINIDO EM REDE
PSS	PSS-04	IMAGENS PARA MÁQUINAS VIRTUAIS E CONTAINERS
PSS	PSS-05	LOCALIZAÇÃO DE TRATAMENTO E ARMAZENAMENTO DE DADOS

17. Anexo II - Requisitos de Segurança com Nível de Garantia Básico

Ref.1	Ref.2	Descrição
OIS	OIS-01.1	O CSP deve definir, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI), contemplando, pelo menos, as unidades operacionais, locais e processos para fornecer o serviço cloud
OIS	OIS-01.4	O CSP deve definir e documentar as medidas para documentar, implementar, manter e melhorar continuamente o SGSI
OIS	OIS-02.1	O CSP deve realizar uma avaliação de risco, tal como definido na RM-01 sobre a acumulação de responsabilidades ou tarefas em papéis ou indivíduos, em relação à prestação de serviço cloud
OIS	OIS-02.2	A avaliação de risco deve contemplar, pelo menos, as seguintes áreas, na medida em que estas são aplicáveis para a prestação de serviço *cloud* e estão na área de responsabilidade do CSP: Administração de perfis, aprovação e atribuição de acessos e autorizações de acesso (cf. IAM-01); Desenvolvimento, teste e *release* de alterações (cf. DEV-01, CCM-01); e Operação dos componentes do sistema .
OIS	OIS-02.3	O CSP deve implementar as medidas de mitigação definidas na avaliação de risco, privilegiando a separação de funções, a menos que seja impossível por razões organizacionais ou técnicas, caso em que as medidas devem incluir a monitorização das atividades a fim de detetar alterações não autorizadas ou não intencionais, bem como uso indevido e as ações apropriadas subsequentes
OIS	OIS-03.1	O CSP deve manter-se informado sobre as ameaças e vulnerabilidades atuais
OIS	OIS-04.1	O CSP deve incluir a segurança da informação na gestão de projetos de todos os projetos que podem afetar o serviço, independentemente da natureza do projeto
ISP	ISP-01.1	O CSP deve documentar uma política global de segurança da informação contemplando, pelo menos, os seguintes aspetos: a importância da segurança da informação, com base nos requisitos dos clientes da *cloud* em relação à segurança da informação, bem como na necessidade de garantir a segurança das informações processadas e armazenadas pelo CSP e dos ativos que suportam os serviços prestados os objetivos de segurança e os níveis adequados e desejados de segurança, com base nos objetivos do negócios e tarefas do CSP; o compromisso do CSP em implementar as medidas de segurança necessárias para atingir os objetivos de segurança estabelecidos; os aspetos mais importantes da estratégia de segurança para alcançar os objetivos de segurança estabelecidos; e a estrutura organizacional de segurança da informação na área de aplicação do SGSI.
ISP	ISP-01.2	A gestão de topo do CSP deve aprovar e fazer o *endorsement* da política global de segurança da informação
ISP	ISP-01.5	O CSP deve comunicar e disponibilizar a política global de segurança da informação para colaboradores internos e externos e para clientes de serviços cloud
ISP	ISP-02.1	O CSP deve derivar políticas e procedimentos da política global de segurança da informação para todos os assuntos relevantes, documentados de acordo com uma estrutura uniforme, incluindo pelo menos os seguintes aspetos: Objetivos; Alcance; Funções e responsabilidades dentro da organização; Funções e dependências de outras organizações (especialmente clientes da cloud e organizações de subserviços); Passos para a execução da segurança estratégia; e Requisitos legais e regulamentares aplicáveis.
ISP	ISP-02.3	O CSP deve comunicar e disponibilizar as políticas e procedimentos a todos os colaboradores internos e externos
ISP	ISP-02.4	A gestão de topo do CSP deve aprovar as políticas e procedimentos de segurança ou delegar essa responsabilidade a órgãos autorizados
ISP	ISP-02.6	Os especialistas do CSP devem rever as políticas e procedimentos para a sua adequação à atualidade, pelo menos anualmente, quando a política global de segurança da informação é atualizada, e quando grandes mudanças podem afetar a segurança do serviço *cloud*
ISP	ISP-02.7	Após uma atualização de procedimentos e políticas, que deverão ser aprovados antes que se tornem efetivos, e, em seguida, comunicados e disponibilizados a todos os colaboradores internos e externos
ISP	ISP-03.1	O CSP deve manter uma lista de exceções às políticas e procedimentos de segurança, incluindo os controlos associados
ISP	ISP-03.2	As exceções são limitadas no tempo
ISP	ISP-03.5	A lista de exceções deve ser revista pelo menos anualmente
RM	RM-01.1	O CSP deve documentar as políticas e procedimentos de acordo com o ISP-02 para os seguintes aspetos: Identificação de riscos associados à perda de confidencialidade, integridade, disponibilidade e autenticidade das informações dentro do âmbito do SGSI e atribuir responsáveis de risco; Análise da probabilidade e impacto de ocorrência e determinação do nível de risco; Avaliação da análise de risco baseada nos critérios definidos de aceitação e priorização de tratamento; Tratamento dos riscos através de medidas, incluindo a aprovação da autorização e aceitação dos riscos residuais pelos responsáveis de risco; e Documentação das atividades implementadas para permitir resultados consistentes, válidos e comparáveis.
RM	RM-02.1	O CSP deve implementar as políticas e procedimentos contemplando avaliações de risco sobre a todo perímetro do serviço *cloud*.
RM	RM-02.2	O CSP deve disponibilizar os resultados da avaliação de risco para todas as partes interessadas
RM	RM-02.3	O CSP deve analisar e rever a avaliação de riscos pelo menos anualmente, e depois de cada grande mudança que pode afetar a segurança do serviço *cloud*.

RM	RM-03.1	O CSP deve priorizar os riscos de acordo com sua criticidade
RM	RM-03.2	O CSP deve definir e implementar um plano para tratar riscos de acordo com seu nível de prioridade, reduzindo ou evitando-os através de controlos de segurança, pela partilha ou retenção
RM	RM-03.3	O plano de tratamento de risco deve reduzir o nível de risco a um limite que os responsáveis do risco considerem aceitável (Risco residual).
RM	RM-03.5	O CSP deve disponibilizar o plano de tratamento para as partes interessadas
RM	RM-03.6	Se o CSP partilha riscos com o CSC, os riscos partilhados devem ser associados aos Controlos Complementares do Cliente (CCCs) e descritos na documentação do utilizador
RM	RM-03.7	O CSP deve rever o plano de tratamento de risco sempre que a avaliação de risco for revista.
HR	HR-01.1	O CSP deve classificar as funções sensíveis à segurança da informação de acordo com seu nível de risco, incluindo funções relacionadas à administração TIC e à prestação do serviço *cloud* no ambiente de produção, e todas as funções com acesso a dados de clientes *cloud* ou componentes de sistema.
HR	HR-01.2	O CSP deve incluir nos seus contratos de trabalho ou num código de conduta ou ética dedicado, um clausulado abrangente para colaboradores internos e externos agirem de forma ética nas suas responsabilidades e funções profissionais.
HR	HR-01.3	O CSP deve documentar, comunicar e implementar uma política que descreva as ações a serem tomadas em caso de violações de políticas e instruções ou requisitos legais e regulamentares aplicáveis, incluindo pelo menos os seguintes aspetos: Verificação se a violação ocorreu; e Consideração da natureza e severidade da violação e o seu impacto.
HR	HR-01.4	Se as medidas disciplinares estiverem definidas na política mencionada no HR-01.3, os colaboradores internos e colaboradores do CSP deve ser informado sobre possíveis medidas disciplinares e o uso destas devem ser devidamente documentadas.
HR	HR-02.2	A competência e integridade de todos os colaboradores internos e externos do CSP com acesso aos dados do cliente cloud ou componentes do sistema sob a responsabilidade do CSP, ou que sejam responsáveis por fornecer o serviço cloud no ambiente de produção, devem ser revistas antes do início do emprego numa função classificada no âmbito do HR-01. A extensão da revisão deve ser proporcional ao contexto de negócio, a sensibilidade da informação que será acedida pelo empregado, e os associados riscos.
HR	HR-03.1	O CSP deve assegurar que todos os colaboradores internos e externos são obrigados nos seus termos e condições de trabalho a cumprir com todas as políticas e procedimentos de segurança da informação aplicáveis.
HR	HR-03.2	O CSP deve assegurar que os termos e condições de trabalho para todos os colaboradores internos e externos incluem disposições de não-divulgação contemplando qualquer informação que tenha sido obtida ou gerada como parte do serviço cloud, mesmo se anónima e descontextualizada.
HR	HR-03.3	O CSP deve fazer uma apresentação de todas as políticas e procedimentos de segurança da informação aplicáveis aos colaboradores internos e externos antes de conceder-lhes qualquer acesso aos dados do cliente, ao ambiente de produção ou a qualquer componente do mesmo
HR	HR-04.1	O CSP deve definir um programa de sensibilização e treino de segurança que cubra os seguintes aspetos: Manusear os componentes do sistema utilizadas para fornecer o serviço cloud no ambiente de produção em conformidade com as políticas e procedimentos aplicáveis; Manipulação de dados de clientes cloud de acordo com as políticas e instruções aplicáveis e requisitos legais e regulamentares aplicáveis; Informações sobre a situação atual de ameaças; e Correto comportamento em evento de incidentes de segurança.
HR	HR-04.3	O CSP deve rever o seu programa de sensibilização e treino de segurança com base nas mudanças nas políticas e instruções e na situação atual de ameaças
HR	HR-04.5	O CSP deve garantir que todos os colaboradores concluam o programa de conscientização e treino de segurança definido para eles
HR	HR-05.1	O CSP deve comunicar aos colaboradores internos e externos as suas responsabilidades relacionadas com a segurança da informação quando seu emprego for rescindido ou alterado
HR	HR-05.2	O CSP deve aplicar um procedimento específico para revogar os direitos de acesso e processar adequadamente as contas e ativos de colaboradores internos e externos quando seu emprego for rescindido ou alterado
HR	HR-06.1	O CSP deve garantir o cumprimento de condições de não-divulgação ou confidencialidade com colaboradores internos, prestadores de serviços externos e fornecedores
AM	AM-01.1	O CSP deve documentar e implementar políticas e procedimentos para manter um inventário de ativos
AM	AM-01.3	O CSP deve registar para cada ativo as informações necessárias à aplicação do procedimento de gestão de risco definido no RM-01
AM	AM-02.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos para uso aceitável e manuseamento seguro de ativos (referência ao ISP-01)
AM	AM-03.1	O CSP deve documentar, comunicar e implementar um procedimento para o comissionamento do hardware que é usado para fornecer o serviço cloud no ambiente de produção, com base nas políticas e procedimentos aplicáveis
AM	AM-03.4	O CSP deve documentar, comunicar e implementar um procedimento para o desmantelamento do hardware que é usado para fornecer o serviço cloud no ambiente de produção, exigindo aprovação de acordo com as políticas aplicáveis
AM	AM-03.5	O procedimento mencionado no AM.03-4 deve incluir a completa e permanente eliminação dos dados ou a destruição adequada dos meios de comunicação.
AM	AM-04.1	O CSP deve garantir e documentar que todos os colaboradores internos e externos estão comprometidos com as políticas e procedimentos no uso aceitável e manuseamento seguro de ativos nas situações descritas em AM-03
AM	AM-04.2	O procedimento mencionado em HR-06.2 deve incluir etapas para garantir que todos os ativos sob custódia de um colaborador sejam devolvidos após o término do contrato de trabalho.

AM	AM-05.1	O CSP deve definir um esquema de classificação de ativos que reflita para cada ativo as necessidades de proteção das informações que processa, armazena ou transmite
AM	AM-05.3	Quando aplicável, o CSP deve classificar todos os ativos de acordo com o esquema de classificação de ativos
PS	PS-01.1	O CSP deve definir perímetros de segurança nos edifícios e instalações relacionadas com a prestação do serviço cloud
PS	PS-01.2	O CSP deve definir no mínimo, duas áreas de segurança; uma contemplando todos os edifícios e instalações e outra com as atividades sensíveis, tais como os edifícios e instalações de armazenamento do sistema de informação para a produção do serviço
PS	PS-01.6	O CSP deve definir e comunicar um conjunto de requisitos de segurança para cada área de segurança numa política de acordo com o SP-02
PS	PS-02.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos relacionados com o controlo de acessos físico às áreas de segurança, de acordo com os requisitos definidos no PS-01 e com base nos princípios definidos no IAM-01
PS	PS-02.2	A política de controlo de acessos deve contemplar o requisito de utilização de pelo menos um fator de autenticação para aceder a qualquer área não pública
PS	PS-02.5	A política de controlo de acessos deve descrever as derrogações de controlos de acesso físico em caso de emergência
PS	PS-02.7	O CSP deve exibir na entrada de todos os perímetros não públicos um aviso sobre os limites e as condições de acesso a esses perímetros
PS	PS-02.8	O CSP deve proteger os perímetros de segurança com medidas de segurança para detetar e prevenir o acesso não autorizado em tempo útil para que ele não comprometa as informações de segurança do serviço cloud
PS	PS-03.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos relativos ao trabalho em áreas não públicas
PS	PS-04.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos relativos à proteção de equipamentos e incluindo, pelo menos, os seguintes aspetos: Proteger a cablagem de energia e comunicação contra interceptações, interferências ou danos; Proteger os equipamentos durante as operações de manutenção Proteger os equipamentos que contêm os dados do cliente durante o transporte.
PS	PS-04.9	O CSP deve usar criptografia nos dispositivos removíveis e de backup aquando da sua deslocação entre áreas de segurança, de acordo com a sensibilidade dos dados armazenados nesses dispositivos.
PS	PS-05.1	O CSP deve documentar e comunicar um conjunto de requisitos de segurança relacionados com ameaças externas e ambientais numa política de acordo com a SP-02, endereçando os seguintes riscos de acordo com os requisitos legais e contratuais aplicáveis: Falhas no planeamento; Acesso não autorizado; Vigilância insuficiente; Ar condicionado insuficiente; Fogo e fumo; Água; Falha de energia; e Ventilação de ar e de filtragem.
OPS	OPS-01.1	O CSP deve documentar e implementar procedimentos para planear capacidades e recursos (pessoal e recursos TIC), que devem incluir na previsão dos requisitos de capacidade futuros, a fim de identificar tendências de uso e gerir a sobrecarga do sistema
OPS	OPS-01.2	O CSP deve cumprir os requisitos incluídos nos acordos contratuais com os clientes cloud relacionados com a prestação do serviço cloud em caso de estrangulamentos de capacidade ou interrupções de recursos TIC
OPS	OPS-02.1	O CSP deve definir e implementar garantias técnicas e organizacionais para a monitorização do provisionamento e desprovisionamento de serviços cloud para garantir a conformidade com os níveis de serviço acordados
OPS	OPS-03.1	O CSP deve permitir ao CSCs o controlo e monitorização da alocação dos recursos de sistemas atribuídos, se as correspondentes capacidades de nuvem capacidades estiverem expostas para os CSCs
OPS	OPS-04.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos de acordo com o ISP-02 para proteger seus sistemas e seus clientes de malware, contemplando pelo menos os seguintes aspetos: Uso de mecanismos de proteção específicos do sistema; Operar programas de proteção nos componentes do sistema sob a responsabilidade do CSP que são usadas para fornecer o serviço cloud no ambiente de produção; e Operar programas de proteção em equipamentos terminais de colaboradores.
OPS	OPS-05.1	O CSP deve aplicar proteção contra malware, se tecnicamente viável, em todos os sistemas que suportam a prestação do serviço cloud no ambiente de produção, de acordo com políticas e procedimentos
OPS	OPS-06.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos de acordo com o ISP-02 para backup e recuperação de dados
OPS	OPS-07.1	O CSP deve documentar e implementar medidas técnicas e organizacionais para monitorizar a execução de backups de dados de acordo com as políticas e procedimentos definidos no OPS- 06
OPS	OPS-08.1	O CSP deve testar os procedimentos de restauração pelo menos anualmente
OPS	OPS-09.1	O CSP deve transferir os dados de backup para um local remoto ou transportá- los em dispositivos de backup para um local remoto
OPS	OPS-09.2	Quando os dados de backup são transmitidos para um local remoto por meio de uma rede, a transmissão dos dados deve ocorrer de forma criptografada que corresponde ao estado da arte (cf. CKM- 02).
OPS	OPS-10.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos de acordo com o ISP-02 que governam o registo e monitorização de eventos nos componentes do sistema sob sua responsabilidade

OPS	OPS-11.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos de acordo com o ISP-02 que governam o manuseamento seguro de dados derivados
OPS	OPS-12.1	O CSP deve monitorizar os dados de registo a fim de identificar eventos que possam levar a incidentes de segurança, de acordo com os requisitos de registo e monitorização
OPS	OPS-12.2	Eventos identificados devem ser reportados aos departamentos apropriados para avaliação e correção/tratamento.
OPS	OPS-13.1	O CSP deve armazenar todos os dados de registo (logs) de forma agregada e protegendo a sua integridade para que se permita a sua avaliação centralizada
OPS	OPS-13.2	Os registos de dados (logs) deves ser apagados quando não são necessário para a finalidade para a qual eles foram recolhidos
OPS	OPS-13.3	A comunicação entre os ativos a serem registados e os servidores de registo deve ser autenticada e protegida, garantindo a integridade e confidencialidade
OPS	OPS-14.1	Os dados de registo gerados permitem uma identificação inequívoca dos acessos do utilizador ao nível do CSC para suportar a análise no caso de um incidente
OPS	OPS-15.1	O CSP deve restringir o acesso aos componentes do sistema usados para registo e monitoração sob sua responsabilidade apenas a utilizadores autorizados
OPS	OPS-15.2	Alterações na configuração de registo e monitorização devem ser feitas de acordo com as políticas aplicáveis (cf. CCM-01)
OPS	OPS-16.1	O CSP deve monitorizar os componentes do sistema de registo e monitorização sob sua responsabilidade, e deve relatar automaticamente as falhas aos departamentos responsáveis para avaliação e correção/tratamento
OPS	OPS-17.1	O CSP deve documentar, comunicar e implementar de acordo com as políticas e procedimentos do ISP-02, medidas técnicas e organizacionais para garantir a identificação e o tratamento de vulnerabilidades nos componentes do sistema usados para prestar o serviço cloud
OPS	OPS-17.3	O CSP deve usar um sistema de classificação para a avaliação de vulnerabilidades que inclui pelo menos classes de vulnerabilidades "críticas" e "altas"
OPS	OPS-18.1	O CSP deve publicar e manter um registo online público e facilmente acessível de vulnerabilidades conhecidas que afetam o serviço cloud e os ativos fornecidos pelo CSP que os CSCs têm de instalar ou operar sob sua própria responsabilidade
OPS	OPS-18.2	O registo online deve indicar pelo menos as seguintes informações para cada vulnerabilidade: A apresentação da vulnerabilidade através de um sistema de classificação reconhecido e aceite pela indústria; A descrição das opções de tratamento para as vulnerabilidades; Informações sobre a disponibilidade de atualizações ou patches para essa vulnerabilidade; Informações sobre o tratamento ou implementação de patches ou atualizações pela CSP ou CSC, incluindo instruções detalhadas para as operações serem realizadas pelo CSC.
OPS	OPS-18.3	O CSP deve publicar e manter uma lista de apontadores para registos online publicados pelos seus fornecedores e prestadores subcontratados, ou integrar regularmente o conteúdo dos registos relevantes para o serviço cloud na sua própria linha registo (cf. OPS- 18.1)
OPS	OPS-18.4	O CSP deve consultar regularmente os registos online registos online publicados pelos seus fornecedores e prestadores subcontratados, analisar o impacto potencial das vulnerabilidades publicadas no serviço cloud e tratá-los de acordo com o processo de tratamento de vulnerabilidades (cf. OPS-17
OPS	OPS-19.1	O CSP deve realizar testes regulares para detetar vulnerabilidades publicamente conhecidas nos componentes do sistema usados para prestar o serviço cloud, de acordo com as políticas de tratamento de vulnerabilidades (cf. OPS-17)
OPS	OPS-20.1	O CSP deve medir, analisar e avaliar regularmente os procedimentos com os quais vulnerabilidades e incidentes são tratados para verificar sua contínua adequação e eficácia
OPS	OPS-21.1	O CSP deve proteger todos os componentes do sistema que são usados para prestar o serviço cloud sob a sua responsabilidade, de acordo com os padrões e referenciais aceites pela indústria
OPS	OPS-21.2	Os requisitos de proteção para cada componente do sistema devem ser documentados
OPS	OPS-22.1	O CSP deve segregar os dados armazenados e processados do CSC em recursos virtuais e físicos partilhados para garantir a confidencialidade e integridade desses dados, de acordo com os resultados de uma análise de risco (cf. RM-01)
IAM	IAM-01.1	O CSP deve documentar, comunicar e disponibilizar políticas e procedimentos de funções (papeis) e direitos para controlar o acesso aos recursos de informação, de acordo com ISP-02 e com base nos requisitos de negócio e segurança do CSP, de acordo com pelo menos os seguintes aspectoss: Parâmetros a serem considerados para tomada de decisão de controlo de acesso; Atribuição e modificação de direitos de acesso com base nos princípios de "privilégios-mínimos" e da "necessidade de saber"; Uso de um mecanismo baseado em funções para a atribuição de direitos de acesso; Segregação de funções entre gestão, aprovação e atribuição de acessos; Regras dedicadas para utilizadores com acessos privilegiados; Requisitos para a aprovação e documentação da gestão de direitos de acesso.
IAM	IAM-01.2	O CSP deve interligar a política de controlo de acessos definida em IAM-01.1 com a política de controlos de acesso físico definida em PS-02.1, para garantir que o acesso às instalações onde as informações estão localizadas também seja controlado.
IAM	IAM-02.1	O CSP deve documentar as políticas de gestão de contas, de acordo com o ISP- 02, nas quais pelo menos os seguintes aspectos devem ser descritos: Atribuição de nomes de utilizador exclusivos; Definição dos diferentes tipos de contas suportados, e atribuição dos parâmetros de controlo de acesso e funções a serem considerados para cada tipo; Eventos que levam ao bloqueio e revogação de contas.

IAM	IAM-02.4	O CSP deve documentar e implementar procedimentos para gerir contas nominais de utilizadores e direitos de acesso para colaboradores internos e externos que cumpram com o conceito de função e direitos e com as políticas de gestão de contas
IAM	IAM-02.5	O CSP deve documentar e implementar procedimentos para gerir contas não pessoais partilhadas e direitos de acesso associados que cumpram com o conceito de função e direitos e com as políticas de gestão de contas
IAM	IAM-02.6	O CSP deve documentar e implementar procedimentos para gerir contas técnicas e respetivos direitos de acesso aos componentes do sistema envolvidos na operação do serviço cloud que cumpram com o conceito de função e direitos e com as políticas de gestão de contas
IAM	IAM-03.1	O CSP deve definir e implementar um mecanismo automatizado para bloquear contas de utilizadores após um determinado período de tempo
IAM	IAM-03.3	O CSP deve definir e implementar um mecanismo automatizado para bloquear contas de utilizador após um certo número de tentativas de autenticação falhadas
IAM	IAM-04.1	O CSP deve documentar e implementar procedimentos para atribuir, atualizar e revogar os direitos de acesso aos recursos do sistema de informação do serviço cloud de uma conta de utilizador sob sua responsabilidade, e esses procedimentos devem estar em conformidade com o conceito de função e direitos e com as políticas de gestão de contas
IAM	IAM-04.2	O CSP deve documentar e implementar um procedimento para atualizar ou revogar os direitos de acesso de um colaborador interno ou externo quando a sua função e responsabilidade mudarem.
IAM	IAM-05.1	O CSP deve rever os direitos de acesso de todas as contas de utilizador sob a sua responsabilidade pelo menos uma vez por ano para garantir que eles ainda correspondem às necessidades atuais
IAM	IAM-06.4	Contas partilhadas sob a responsabilidade do CSP devem ser atribuídas apenas a colaboradores internos ou externos
IAM	IAM-07.1	O CSP deve documentar e implementar uma política e procedimentos sobre os mecanismos de autenticação, contemplando pelo menos os seguintes aspectos: A seleção de mecanismos adequados para cada tipo de conta e cada nível de risco; A proteção de credenciais utilizadas pelo mecanismo de autenticação; A geração e distribuição de credenciais para novas contas; Regras para a renovação de credenciais, incluindo renovações periódicas, renovações em caso de perda ou compromisso; e Regras sobre a robustez necessária das credenciais, juntamente com mecanismos para comunicar e fazer cumprir as regras.
IAM	IAM-07.7	Todos os mecanismos de autenticação devem incluir um mecanismo para bloquear uma conta após um número predefinido de tentativas mal sucedidas
IAM	IAM-08.1	O CSP deve documentar, comunicar e disponibilizar a todos os utilizadores sob a sua responsabilidade regras e recomendações para a gestão de credenciais, incluindo pelo menos: Não reutilização de credenciais; Contrapartidas entre entropia e capacidade de memorizar; Recomendações para renovação de senhas; Regras de armazenamento de senhas;
IAM	IAM-08.4	As senhas devem ser armazenadas apenas usando funções hash criptograficamente fortes (cf. CKM-01)
IAM	IAM-08.5	Caso sejam utilizados mecanismos de autenticação criptográfica, estes devem seguir as políticas e procedimentos do CKM-01.
IAM	IAM-09.1	O CSP deve implementar medidas de segmentação suficientes entre o sistema de informação que fornece o serviço cloud e os seus outros sistemas de informação
IAM	IAM-09.4	O CSP deve implementar medidas adequadas para a segmentação entre os CSCs
CKM	CKM-01.1	O CSP deve documentar, comunicar, disponibilizar e implementar políticas com garantias técnicas e organizacionais para a criptografia e gestão de chaves, de acordo com o ISP-02, nas quais pelo menos os seguintes aspectos deverão ser descritos: Uso de procedimentos de criptografia forte e protocolos de rede seguros; Requisitos para a criação, armazenamento, arquivo, recuperação, distribuição, cancelamento e apagamento seguro de chaves; Obrigações e requisitos legais e regulamentares relevantes.
CKM	CKM-02.1	O CSP deve definir e implementar mecanismos de criptografia fortes para a transmissão de dados de clientes cloud em redes públicas
CKM	CKM-03.1	O CSP deve documentar e implementar procedimentos e garantias técnicas para criptografar os dados dos clientes cloud durante o armazenamento
CKM	CKM-04.1	Procedimentos e técnicas de garantias para gestão segura de chaves na área de responsabilidade do CSP devem incluir pelo menos os seguintes aspetos: Criação de chaves criptográficas para diferentes sistemas e aplicações; Emissão e obtenção de certificados de chave pública; Provisionamento e ativação das chaves; Armazenamento seguro de chaves, incluindo a descrição de como os utilizadores autorizados obtêm acesso; Alteração ou atualização de chaves criptográficas, incluindo as políticas que definem as condições sob quais e em que forma as alterações e/ou atualizações estão a ser realizadas; Tratamento de chaves comprometidas; e Retirada e exclusão de chaves.
CS	CS-01.1	O CSP deve documentar, comunicar e implementar garantias técnicas que sejam adequadas para detetar e responder de forma apropriada a ataques baseados em rede e para garantir a proteção da informação e dos sistemas de processamento da informação, de acordo com o ISP-02
CS	CS-02.1	O CSP deve documentar, comunicar, disponibilizar e implementar requisitos de segurança específicos para se conectar dentro da sua rede, incluindo pelo menos: quando as zonas de segurança estão a ser separados e quando os clientes cloud estão a ser logicamente ou

		fisicamente segregados; quais relações de comunicação e quais protocolos de rede e aplicativos são permitidos em cada caso; como o tráfego de dados para administração e monitorização é segregado ao nível da rede; que comunicação interna e de cruzamento de localização é permitida; e que comunicação entre redes é permitida.
CS	CS-03.1	O CSP deve distinguir entre redes confiáveis e não confiáveis, com base em uma avaliação de risco
CS	CS-03.2	O CSP deve separar redes confiáveis e não confiáveis em diferentes zonas de segurança para áreas de rede interna e externa (e DMZ, se aplicável)
CS	CS-03.3	O CSP deve projetar e configurar ambientes de rede físicos e virtualizados para restringir e monitorizar a conexão de redes de confiança ou não confiança de acordo com os requisitos de segurança definidos (cf. CS-02)
CS	CS-03.4	O CSP deve rever em intervalos especificados a justificação do negócio para o uso de todos os serviços, protocolos e portas. Esta revisão deve incluir também as medidas compensatórias usadas para protocolos que são considerados inseguros
CS	CS-04.1	Cada perímetro de rede deve ser controlado por *gateways* de segurança
CS	CS-05.1	O CSP deve definir e implementar redes separadas para a gestão administrativa da infraestrutura e o funcionamento das consolas de gestão
CS	CS-05.2	O CSP deve separar lógica ou fisicamente as redes para administração das redes dos CSCs
CS	CS-05.3	O CSP deve segregar física ou logicamente as redes usadas para migrar ou criar máquinas virtuais
CS	CS-06.1	O CSP deve definir, documentar e implementar mecanismos de segregação ao nível de rede do tráfego de dados de diferentes clientes cloud
CS	CS-07.1	O CSP deve manter atualizada toda a documentação da estrutura lógica da rede utilizada para fornecimento ou operação do serviço cloud
CS	CS-07.2	A documentação deve contemplar, pelo menos, como as sub-redes são alocadas, como a rede é segmentada em zonas, como é que ela estabelece ligação+D307 a redes públicas e de terceiros e as localizações geográficas nas quais os dados dos clientes cloud são armazenados
CS	CS-08.1	O CSP deve garantir a confidencialidade dos dados do utilizador cloud por procedimentos adequados ao oferecer funções para redes definidas por software (SDN)
CS	CS-08.2	O CSP deve validar a funcionalidade das funções SDN antes de fornecer novos recursos SDN aos CSCs ou modificar os recursos SDN existentes
CS	CS-09.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos com garantias técnicas e organizacionais para proteger a transmissão de dados contra interceção, manipulação, cópia, modificação, redireccionamento ou destruição não autorizada, de acordo com o ISP-02
PI	PI-01.1	O serviço cloud deve ser acessível por serviços cloud de outros CSPs ou sistemas TIC de clientes cloud por meio de interfaces de entrada e saída documentadas
PI	PI-01.2	As interfaces devem ser claramente documentadas para que os especialistas entendam como podem ser usadas para recuperar os dados
PI	PI-01.3	A comunicação nessas interfaces deve usar protocolos de comunicação padronizados que garantam a confidencialidade e integridade das informações transmitidas de acordo com os seus requisitos de proteção
PI	PI-01.4	A comunicação em redes não confiáveis deve ser criptografada de acordo com CKM-02
PI	PI-02.1	O CSP deve incluir nos acordos contratuais do serviço cloud, pelo menos, os seguintes aspectos relativos à rescisão do contratual: Tipo, âmbito e formato dos dados que o CSP fornece para o CSC; Métodos de entrega dos dados ao cliente cloud; Definição do período de tempo, dentro do qual o CSP disponibiliza os dados ao CSC; Definição do momento a partir do qual o CSP torna os dados inacessíveis para o CSC e os elimina; e As responsabilidades e obrigações do CSC para cooperar no fornecimento dos dados.
PI	PI-03.1	O CSP deve implementar procedimentos para eliminação de dados dos seus clientes após a rescisão dos seus contratos, em conformidade com os acordos contratuais existentes
PI	PI-03.2	A eliminação de dados do CSC deve incluir também metadados e dados armazenados nos backups
CCM	CCM-01.1	O CSP deve documentar, implementar, e comunicar as políticas e procedimentos para a gestão de alterações dos sistemas TIC que suportam o serviço cloud de acordo com a ISP-02
CCM	CCM-02.1	O CSP deve categorizar e priorizar as alterações, considerando os potenciais efeitos de segurança nos componentes do sistema em questão
CCM	CCM-03.1	O CSP deve testar as alterações propostas antes da sua implementação
CCM	CCM-04.1	O CSP deve aprovar qualquer alteração no serviço cloud, de acordo com critérios definidos, antes de serem disponibilizados aos CSCs no ambiente de produção
CCM	CCM-05.1	O CSP deve definir direitos e funções de acordo com IAM-01 para pessoas autorizadas ou componentes do sistema que têm permissão para fazer alterações no serviço cloud em ambiente de produção.
CCM	CCM-05.2	Todas as alterações no serviço cloud no ambiente de produção devem ser registadas e devem ser rastreáveis tendo em consideração a pessoa ou componente do sistema que iniciou a alteração
CCM	CCM-06.1	O CSP deve implementar procedimentos de controlo de versões para rastrear as dependências de alterações individuais e para restaurar os componentes do sistema afetados ao seu estado anterior, como resultado de erros ou vulnerabilidades identificadas.
DEV	DEV-01.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos de acordo com o ISP-02 com medidas técnicas e organizacionais para o desenvolvimento seguro do serviço cloud.
DEV	DEV-01.2	As políticas e procedimentos para o desenvolvimento seguro devem considerar a segurança da informação desde as primeiras fases do projeto
DEV	DEV-02.1	O CSP deve manter uma lista de dependências de produtos de hardware e software usados no desenvolvimento do seu serviço cloud

DEV	DEV-03.1	O CSP deve assegurar que a confidencialidade e integridade do código fonte é protegido adequadamente em todos os estágios de desenvolvimento
DEV	DEV-03.2	O CSP deve usar o controlo de versões para manter um histórico das alterações no código-fonte com a atribuição de alterações aos programadores, a título nominal.
DEV	DEV-04.1	O CSP deve assegurar que os ambientes de produção são fisicamente ou logicamente separados dos ambientes de desenvolvimento, teste ou pré-produção
DEV	DEV-04.2	Os dados contidos nos ambientes de produção não devem ser utilizados nos ambientes de desenvolvimento, teste ou pré-produção para não comprometer sua confidencialidade
DEV	DEV-05.1	O CSP deve documentar, comunicar, disponibilizar e implementar procedimentos específicos para o desenvolvimento de funções que implementem mecanismos técnicos ou garantias exigidas pelo esquema EUCS, com requisitos de teste acrescidos.
DEV	DEV-06.1	O CSP deve aplicar medidas apropriadas para verificar vulnerabilidades que podem ter sido integradas no serviço cloud durante o processo de desenvolvimento.
DEV	DEV-06.2	Os procedimentos para identificação de vulnerabilidades devem ser integrados no processo de desenvolvimento.
DEV	DEV-07.1	Quando o desenvolvimento do serviço cloud ou componentes do mesmo é subcontratado a um terceiro, o CSP e o contratado devem acordar contratualmente as especificações, pelo menos, em relação aos seguintes aspectos: Segurança no desenvolvimento de software (requisitos, desenho, implementação, testes e verificações) de acordo com normas, referenciais e métodos reconhecidos; Aceitação de testes da qualidade dos serviços prestados em conformidade com os requisitos funcionais e não funcionais acordados; e Providenciar evidências que suficientes verificações foram levadas a cabo para excluir a existência de vulnerabilidades conhecidas.
PM	PM-01.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos de acordo com o ISP-02 para controlar e monitorizar terceiras partes cujos produtos ou serviços contribuem para a prestação do serviço cloud
PM	PM-02.1	O CSP deve realizar uma avaliação de risco dos seus fornecedores de acordo com as políticas e procedimentos para o controlo e monitorização de terceiros antes dos mesmos contribuírem para a prestação do serviço cloud.
PM	PM-02.3	Após a avaliação de risco de um prestador de serviço, o CSP deve definir, para cada requisito aplicável do EUCS, uma listagem dos controlos organizacionais complementares ao subserviço (CSOC), a serem implementado pelo prestador
PM	PM-02.4	O CSP deve garantir que o prestador de serviços tem implementado os CSOCs, e que este disponibiliza evidências que apoiem a avaliação da sua eficácia para o nível de avaliação requerido
PM	PM-02.5	A adequação da avaliação de risco e a definição de CSOCs deve ser revisto regularmente, pelo menos anualmente
PM	PM-03.1	O CSP deve manter um diretório para controlar e monitorizar os fornecedores que contribuem para a prestação do serviço cloud
PM	PM-03.3	O CSP deve verificar o diretório quanto à sua integridade, precisão e validade, pelo menos, anualmente
PM	PM-04.1	O CSP deve monitorizar a conformidade dos seus fornecedores com os requisitos de segurança da informação e requisitos legais e regulamentares aplicáveis, de acordo com as políticas e procedimentos relativos ao controlo e monitorização de terceiros
PM	PM-04.3	A frequência da monitorização deve corresponder à classificação baseada na avaliação de riscos do terceiro realizada pelo CSP (cf. PM-02), e os resultados da monitorização devem ser incluídos na revisão da avaliação de risco desta terceira parte.
PM	PM-04.4	As violações e desvios identificados devem ser analisados, avaliados e tratados de acordo com o procedimento de gestão de risco (cf. RM-01)
PM	PM-04.5	Quando uma alteração num terceiro contribui para a entrega do serviço cloud afeta o seu nível de segurança, o CSP deve informar todos de seus CSCs, sem demora
PM	PM-05.1	O CSP deve definir estratégias de saída para a compra de serviços onde a avaliação de risco dos fornecedores identificou uma dependência muito alta
IM	IM-01.1	O CSP deve documentar, comunicar e implementar políticas e procedimentos de acordocom o ISP-02 contendo garantias técnicas e organizacionais para garantir uma resposta rápida, eficaz e adequada a todos os incidentes de segurança conhecidos.
IM	IM-01.2	As políticas e procedimentos devem incluir diretrizes para a classificação, priorização e escalonamento de incidentes de segurança e criar interfaces para gestão de incidentes e gestão de continuidade de negócios
IM	IM-01.3	O CSP deve estabelecer uma Equipa de Resposta a Incidentes (CSIRT), que contribua para a resolução coordenada de incidentes de segurança
IM	IM-02.1	O CSP deve classificar, priorizar e realizar análises de causa raiz para eventos que possam constituir um incidente de segurança, recorrendo a especialistas ou a prestadores de segurança externos, quando apropriado.
IM	IM-03.1	O CSP deve documentar as medidas implementadas após o tratamento de um incidente de segurança e, na sequência dos acordos contratuais, o documento deve ser enviado aos clientes afetados para conhecimento final ou, se aplicável, como confirmação.
IM	IM-03.2	O CSP deve disponibilizar informações sobre incidentes de segurança ou violações de segurança confirmadas a todos os clientes afetados
IM	IM-04.1	O CSP deve informar os colaboradores e parceiros de negócio das suas obrigações contratuais, de forma a relatar todos os eventos de segurança que são conhecidos pelos mesmos e estão diretamente relacionados com o serviço cloud
IM	IM-04.2	O CSP não deve tomar qualquer ação negativa contra aqueles que comunicam " relatórios falsos" de eventos que posteriormente não se transformem em incidentes, e deve tornar essa política conhecida como parte de sua comunicação aos colaboradores e parceiros de negócio
IM	IM-04.3	O CSP deve definir, disponibilizar publicamente e implementar um único ponto de contato para reportar eventos de segurança e vulnerabilidades

IM	IM-05.1	O CSP deve informar periodicamente os seus clientes sobre a situação dos incidentes que afetam o CSC, ou, quando apropriado e necessário, envolvê-los na resolução, de acordo com os acordos contratuais
IM	IM-05.2	Assim que um incidente for resolvido, o CSP deve informar os seus clientes sobre as ações tomadas, de acordo com os acordos contratuais
IM	IM-06.1	O CSP deve realizar uma análise de incidentes de segurança para identificar incidentes recorrentes ou significativos e para identificar a necessidade de proteção adicional, com o apoio de órgãos externos, se necessário.
IM	IM-06.2	O CSP só deve contratar órgãos externos de apoio que sejam prestadores de serviços de resposta a incidentes qualificados ou agências governamentais
IM	IM-07.1	O CSP deve documentar e implementar um procedimento para arquivar todos os documentos e evidências que forneçam detalhes sobre incidentes de segurança
IM	IM-07.4	O CSP deve aplicar mecanismos e processos de segurança para proteger toda a informação relacionada com incidentes de segurança, em conformidade com os níveis de criticidade e requisitos legais em vigor
BC	BC-01.1	O CSP deve documentar, comunicar e disponibilizar políticas e procedimentos que estabelecem a estratégia e diretrizes para garantir a continuidade de negócio e gestão de contingências
BC	BC-02.1	As políticas e procedimentos para a gestão de continuidade de negócio e de crises deve incluir a necessidade de realizar uma análise de impacto de negócio para determinar o impacto de qualquer mau funcionamento para serviço cloud ou organização.
BC	BC-03.1	O CSP deve documentar e implementar um plano de continuidade de negócio e contingência para assegurar a continuidade dos serviços, tendo em consideração restrições de segurança da informação de contas e os resultados da análise de impacto do negócio.
CO	CO-01.1	O CSP deve documentar os requisitos legais, regulatórios, auto-impostos e contratuais relevantes para a segurança da informação do serviço cloud.
CO	CO-02.1	O CSP deve documentar, comunicar, disponibilizar e implementar políticas e procedimentos para planeamento e realização de auditorias, feitas de acordo com o ISP-02 e abordando, no mínimo, os seguintes aspetos: Restrição para acessos apenas de leitura aos componentes dos sistemas, em conformidade com o plano de auditoria acordado, e com o necessário para realizar as atividades; Atividades que podem resultar em mau funcionamento do serviço cloud ou violações de requisitos contratuais são realizadas durante as janelas de manutenção programada ou fora dos períodos de pico; e Registo e monitorização das atividades.
CO	CO-03.1	O CSP deve realizar em intervalos regulares e pelo menos anualmente auditorias internas por especialistas para verificar o cumprimento do seu sistema interno de controlos de segurança face aos requisitos definidos no CO-01.
CO	CO-03.2	A auditoria interna deve verificar a conformidade com os requisitos do esquema EUCS assegurando o respetivo nível de garantia.
CO	CO-03.6	O CSP deve documentar especificamente os desvios que são não-conformidades com os requisitos da EUCS, incluindo uma avaliação da sua gravidade e acompanhar a sua correção
CO	CO-04.1	O CSP deve informar regularmente a sua gestão de topo sobre o desempenho da segurança da informação dentro do âmbito e sistema de controlo interno.
DOC	DOC-01.1	O CSP deve disponibilizar publicamente as diretrizes e recomendações para auxiliar os CSCs com a configuração, instalação, implementação, operação e manutenção seguras da prestação do serviço cloud.
DOC	DOC-01.3	O CSP deve manter orientações e recomendações aplicáveis ao serviço cloud na versão destinada ao uso produtivo
DOC	DOC-02.1	O CSP deve operar ou disponibilizar ao público um registo online atualizado diariamente de vulnerabilidades conhecidas que afetam a prestação do serviço cloud
DOC	DOC-03.1	O CSP deve fornecer informações compreensíveis e transparentes sobre: Sua jurisdição; e Localização de componentes do sistema, incluindo os seus subcontratados, onde os dados do cliente cloud são tratados, armazenados e submetidos a backup.
DOC	DOC-03.2	O CSP deve fornecer informação suficiente a especialistas do CSC para determinar e avaliar a adequação da jurisdição do serviço cloud e localização de uma perspetiva legal e regulamentar.
DOC	DOC-04.1	O CSP deve apresentar uma justificação para o nível de garantia a alcançar na certificação, com base nos riscos associados aos serviços cloud direcionados aos utilizadores e casos de uso
DOC	DOC-04.2	Se o CSP alegar conformidade com perfis de segurança para a sua prestação de serviços cloud, a justificação deve abranger os perfis de segurança.
DOC	DOC-04.3	Um resumo da justificação devem ser disponibilizado publicamente como parte do pacote de certificação, que deve permitir aos CSCs executar uma análise de alto nível sobre os seus próprios casos de uso
DOC	DOC-05.1	Se o CSP espera que os CSCs certifiquem com EUCS os seus próprios serviços baseados no seu serviço cloud usando composição, deve fornecer documentação específica para estes, com base nos Controlos Complementares do Utilizador (CCCs) que eles têm definidos
DOC	DOC-05.2	O CSP deve incluir na descrição fornecida para cada CCC uma lista de requisitos acionáveis para o CSC, e que associa cada CCC para um requisito EUCS
DOC	DOC-05.3	O CSP deve disponibilizar a documentação definida no DOC-05.1 aos clientes cloud mediante solicitação
DOC	DOC-06.1	Se o CSP espera que os CSCs certifiquem com EUCS os seus próprios serviços com base no seu serviço cloud usando composição, ele deve documentar para cada requisito de EUCS como seu serviço em nuvem contribuirá (se houver) para o cumprimento do requisito pelo serviço em nuvem desenvolvido pela CSC usando o CSP como organização de subserviço
DOC	DOC-06.2	O CSP deve disponibilizar a documentação definida no DOC-06.1 aos clientes cloud, mediante solicitação
DOC	INQ-01.1	O CSP deve sujeitar-se a pedidos de investigação de agências governamentais para uma avaliação legal por especialistas
INQ	INQ-01.2	A avaliação legal deve determinar se a agência governamental tem uma base aplicável e legalmente válida e quais etapas adicionais que precisam ser tomadas

INQ	INQ-02.1	O CSP deve informar os CSC afetado(s), sem atrasos indevidos, a menos que a base legal aplicável sobre a qual a agência governamental se baseia proíbe isso ou há indícios claros de ações ilegais em conexão com o uso do serviço cloud
INQ	INQ-03.1	O CSP só deve fornecer acesso ou divulgar dados do cliente cloud em contextos de pedidos de investigação de agências governamentais após a avaliação legal do CSP (cf. INQ-01) ter mostrado que existe uma base legal aplicável e válida e que a solicitação de investigação deve ser concedida segundo essa base.
INQ	INQ-03.2	O CSP deve documentar e implementar procedimentos para garantir que as agências governamentais só tenham acesso aos dados que precisam para investigação
INQ	INQ-03.4	O CSP deve monitorizar automaticamente os acessos realizados por ou em nome dos investigadores para garantir que correspondem à base legal determinada
PSS	PSS-01.1	O CSP deve oferecer aos seus CSCs mecanismos de gestão e registo (logs) de erros que lhes permitam obter informações relacionadas com segurança sobre o estado (status) de segurança do serviço cloud, bem como os dados, serviços ou funções que ele fornece
PSS	PSS-02.1	Deve ser usado um sistema de gestão de sessões adequado que corresponda, pelo menos, ao estado de arte e seja protegido contra ataques conhecidos
PSS	PSS-03.1	O CSP deve garantir a confidencialidade dos dados do utilizador cloud através de procedimentos adequados quando oferece funções para redes definidas por software (SDN)
PSS	PSS-03.2	O CSP deve validar a funcionalidade das funções SDN antes de fornecer novos recursos SDN aos CSCs ou modificar os recursos SDN existentes
PSS	PSS-04.1	O CSP deve garantir os seguintes aspetos se os CSCs operarem máquinas virtuais ou containers com o serviço cloud: O CSC pode restringir a seleção de imagens das máquinas virtuais ou containers de acordo com suas especificações, de forma que os utilizadores deste CSC só podem lançar as imagens ou containers disponibilizados de acordo com essas restrições. Além disso, essas imagens fornecidas pelo CSP são reforçadas de acordo com os padrões e referências geralmente aceites pela indústria.

(os requisitos a sombreado estão diretamente relacionados com o EUCS)

18. Anexo III - Requisitos de Segurança com Nível de Garantia Substancial

Ref.1	Ref.2	Descrição
OIS	OIS-01.2	O SGSI deve estar de acordo com a ISO / IEC 27001
OIS	OIS-03.2	O CSP deve manter contatos com as autoridades competentes em termos de segurança da informação e grupos técnicos relevantes para se manter informado sobre as ameaças e vulnerabilidades atuais
OIS	OIS-04.2	O CSP deve realizar uma avaliação de risco de acordo com a RM-01 para avaliar e tratar os riscos em qualquer projeto que podem afetar a prestação do serviço *cloud*
ISP	ISP-01.3	O CSP deve rever a política global de segurança da informação, pelo menos, após qualquer mudança organizacional significativa suscetível de afetar os princípios definidos na política, incluindo a aprovação e endorsement pela gestão de topo.
ISP	ISP-02.2	As políticas e procedimentos devem incluir requisitos de qualificação de pessoal e o estabelecimento de regras de substituição na sua descrição de funções e responsabilidades dentro da organização
ISP	ISP-03.3	As exceções deverão ser contempladas no processo de gestão de risco RM-01, incluindo a aprovação destas exceções e aceitação dos riscos associados pelos responsáveis
ISP	ISP-03.6	As aprovações da lista de exceções devem ser reiteradas pelo menos anualmente, mesmo se a lista não tiver sido atualizada
RM	RM-01.2	O CSP deve usar um método de análise de risco documentado que garanta a reprodutibilidade e comparabilidade da abordagem
RM	RM-03.4	Os responsáveis do risco devem aprovar formalmente o plano de tratamento e, em particular, aceitar o risco residual
RM	RM-03.8	Os responsáveis do risco devem rever adequadamente a análise, avaliação e tratamento de riscos, incluindo a aprovação de ações e aceitação de riscos residuais, após cada revisão da avaliação de risco e planos de tratamento
HR	HR-02.3	A competência e integridade dos colaboradores internos e externos do CSP deve ser revista antes do início do emprego numa função com uma classificação de risco mais elevada do que sua função/atividade/posição anterior
HR	HR-03.4	Todos os colaboradores internos e externos devem reconhecer, na forma documentada, as políticas e procedimentos de segurança de informação que lhes são apresentados antes de ser concedido qualquer acesso aos dados do cliente, ao ambiente de produção, ou qualquer componente do mesmo
HR	HR-04.2	O CSP deve definir um programa de sensibilização e treino orientada ao grupo-alvo, levando em consideração, pelo menos, a classificação de risco da função/cargo e deveres técnicos
HR	HR-04.4	O CSP deve atualizar o seu programa de sensibilização e treino de segurança pelo menos anualmente
HR	HR-04.6	O CSP deve garantir que todos os colaboradores concluam o programa de sensibilização e treino de segurança numa base regular, e quando muda o público-alvo
HR	HR-04.8	O CSP deve medir e avaliar os resultados da aprendizagem alcançados através do programa de sensibilização e treino de segurança
HR	HR-04.10	O CSP deve verificar a eficácia do programa de sensibilização e treino de segurança utilizando exercícios práticos que simulam ataques de cibersegurança reais
HR	HR-05.3	O procedimento mencionado em HR-05.2 deve definir funções e responsabilidades específicas e incluir uma lista de verificação documentada de todas as etapas necessárias
HR	HR-06.2	Os acordos de não divulgação ou confidencialidade devem basear-se nos requisitos identificados pelo CSP para a proteção da confidencialidade de informação e detalhes operacionais
HR	HR-06.3	Os acordos devem ser aceites por prestadores de serviços externos e fornecedores quando o contrato for assinado
HR	HR-06.4	Os acordos devem ser aceites por colaboradores internos do CSP antes de ser atribuída autorização para aceder a dados de clientes cloud.
HR	HR-06.5	Os requisitos nos quais os acordos se baseiam devem ser documentados e revisto em intervalos regulares, pelo menos anualmente; se a análise mostrar que os requisitos precisam ser adaptados, os acordos de não divulgação ou confidencialidade devem ser atualizados em conformidade.
HR	HR-06.6	O CSP deve informar os seus colaboradores internos, prestadores de serviços externos e fornecedores e obter a confirmação da atualização dos acordos de não divulgação ou confidencialidade.
AM	AM-01.2	O inventário deverá ser realizado automaticamente e/ou por pessoas ou equipas responsáveis para garantir um inventário de ativos completo, preciso, válido e consistente em todo o seu ciclo de vida.
AM	AM-01.4	A informação registada com os ativos deve incluir as medidas tomadas para gerir os riscos associados ao ativo ao longo do seu ciclo de vida
AM	AM-02.2	As políticas e procedimentos para uso aceitável e manuseamento seguro de ativos deve endereçar, pelo menos, os seguintes aspetos do ciclo de vida do ativo (referência ao ISP- 01)
AM	AM-03.2	O procedimento mencionado em AM-03.1 deve garantir que os riscos decorrentes do comissionamento são identificados, analisados e mitigados.
AM	AM-03.3	O procedimento mencionado em AM-03.1 deve incluir a verificação da configuração segura dos mecanismos de tratamento de erros, registo (logging), criptografia, autenticação e autorização de acordo com o uso pretendido e com base nas políticas aplicáveis, antes da autorização para comissionar o ativo possa ser concedida.
AM	AM-05.2	O esquema de classificação de ativos deve fornecer níveis de proteção de acordo com os objetivos de confidencialidade, integridade, disponibilidade e autenticidade.
AM	AM-05.4	A necessidade de proteção deve ser determinada pelos indivíduos ou grupos responsáveis pelos ativos
PS	PS-01.7	Os requisitos de segurança em PS-01.5 devem ser baseados nos objetivos de segurança da política de segurança da informação, nos requisitos de proteção identificados para o serviço cloud e na avaliação de riscos à segurança física e ambiental

PS	PS-02.3	A política de controlo de acessos deve contemplar o requisito de utilização de pelo menos dois fatores de autenticação para acesso às áreas sensíveis e de alojamento das componentes do sistema componentes que processam dados dos clientes cloud
PS	PS-02.4	A política de controlo de acessos deve incluir medidas para controlar individualmente os visitantes e pessoal terceiro durante o seu trabalho nas instalações e edifícios, identificando-os e supervisionado durante a sua permanência.
PS	PS-02.9	A política de controlo de acessos deve incluir o registo de todos os acessos a áreas não-públicas para permitir o CSP verificar se só o pessoal definido tem entrado nessas zonas
PS	PS-03.2	As políticas e procedimentos em PS-02.1 devem incluir uma política de ecrã limpo e uma política de mesa limpa para documentos e dispositivos removíveis
PS	PS-04.2	Os procedimentos definidos em PS-04.1 devem incluir um procedimento de verificação da proteção da cablagem de energia e comunicações, a ser realizado regularmente, no mínimo a cada dois anos, bem como em casos de suspeita de manipulação por pessoal qualificado
PS	PS-04.3	As políticas e procedimentos em PS-04.1 devem incluir um procedimento para a transferência de qualquer equipamento que contenha dados de clientes fora do local (off-site) para descarte que garanta que o nível de proteção em termos de confidencialidade e integridade dos ativos durante o seu transporte é equivalente ao que no local (on-site)
PS	PS-05.2	Os requisitos de segurança definidos no PS-05.1 para datacenters devem ser baseados em critérios que atendam às regras de tecnologia estabelecidas
PS	PS-05.5	O CSP deve fornecer o serviço cloud a partir de pelo menos dois locais separados por uma distância adequada e que proporcionem redundância ou resiliência operacional em relação um ao outro
PS	PS-05.6	O CSP deve verificar a eficácia da redundância pelo menos uma vez um ano através de testes e exercícios adequados (cf. BCM-04)
OPS	OPS-04.2	O CSP deve criar relatórios regulares sobre as verificações de malware realizadas, que deverão ser revistos e analisados por orgãos autorizados nas revisões das políticas relacionadas com malwares
OPS	OPS-05.2	Ferramentas de proteção contra malware baseadas em assinatura e comportamentos devem ser atualizadas pelo menos diariamente
OPS	OPS-06.2	As políticas e procedimentos para backup e recuperação devem contemplar pelo menos os seguintes aspectos: A extensão e frequência dos backups de dados e a duração da retenção de dados são conformes com os acordos contratuais com os clientes cloud e os requisitos de continuidade operacional do CSP para o Objetivo do Tempo de Recuperação (RTO - Recovery Time Objective) e o Objetivo do Ponto de Recuperação (RPO - Recovery Point Objective); Existe redundância (back-up) de dados com recurso a encriptação estado-da-arte; Acesso aos backups de dados e a execução de restaurações é realizada unicamente por pessoas autorizadas; e Testes de procedimentos de recuperação (cf. OPS-08).
OPS	OPS-08.2	Os testes de restauração devem avaliar se as especificações para o RTO e RPO acordadas com os clientes são atendidas
OPS	OPS-08.3	Qualquer desvio da especificação durante os testes de restauração deve ser reportado para o responsável do CSP para avaliação e correção/tratamento
OPS	OPS-09.3	O CSP deve selecionar um local remoto para armazenar os backups tendo em consideração a distância, tempos de recuperação e o impacto de desastres de ambos os locais
OPS	OPS-09.4	As medidas de segurança física e ambiental no local remoto devem ter o mesmo nível que a do local principal
OPS	OPS-10.2	As políticas e procedimentos devem contemplar pelo menos os seguintes aspetos: Definição de eventos que podem levar a uma violação dos objetivos de proteção; Especificações para ativar, parar e colocar em pausa os vários registos (logs); Informações sobre a finalidade e período de retenção dos registos (logs); Definição dos papéis e responsabilidades para o estabelecimento e monitorização de registos (logs); Sincronização de tempo dos componentes do sistema; e Conformidade com quadros legais e regulatórios
OPS	OPS-11.2	As políticas e procedimentos sobre dados derivados devem cobrir pelo menos os seguintes aspetos: Finalidade da recolha e uso de dados derivados além da operação do serviço cloud, incluindo os fins relacionados com a a implementação de controlos de segurança; Anonimização dos dados sempre que são utilizados num contexto que vai além de um único CSC; Período de armazenamento relacionado para os fins da recolha; Garantia de eliminação quando as finalidades de recolha forem cumpridas e o armazenamento posterior não for necessário; e Provisão dos dados derivados de CSCs de acordo com os acordos contratuais.
OPS	OPS-11.3	O CSP deve listar no acordo contratual todos os fins de recolha de uso de dados derivados que são não estejam relacionados com a implementação de controlos de segurança ou para faturação
OPS	OPS-12.3	A monitorização dos eventos mencionados no OPS-12.1 deve ser automatizada
OPS	OPS-13.4	A comunicação entre os ativos a serem registados e os servidores de registo deve ser criptografada usando criptografia de estado de arte ou deve ser feita através de uma rede de administração dedicada
OPS	OPS-13.5	O CSP deve implementar procedimentos suportados tecnicamente para cumprir os requisitos relacionados com o acesso, armazenamento e eliminação das seguintes restrições: Acesso apenas a utilizadores e sistemas autorizados; Retenção para um período específico; e Eliminação quando a retenção já não necessária para a finalidade de recolha.
OPS	OPS-14.2	O CSP deve disponibilizar interfaces para realizar análises forenses e realizar backups de componentes de infraestrutura e a sua comunicação de rede
OPS	OPS-15.3	O acesso aos componentes do sistema para registo e monitorização deve contemplar autenticação forte

OPS	OPS-17.2	As políticas e procedimentos devem descrever medidas contemplando, pelo menos, aos seguintes aspetos: Identificação regular de vulnerabilidades; Avaliação da severidade das vulnerabilidades identificadas; Priorização e implementação de ações para corrigir ou mitigar prontamente as vulnerabilidades identificadas com base na sua severidade e de acordo com os prazos definidos; e Tratamento de componentes do sistema para os quais nenhuma medida de correção ou mitigação de vulnerabilidades foi iniciada em tempo útil.
OPS	OPS-17.4	O CSP deve mandatar nas suas políticas e procedimentos o tratamento imediato de vulnerabilidades “críticas” e o tratamento de vulnerabilidades “altas” dentro de um dia, havendo um acompanhamento da vulnerabilidade até que ela tenha sido corrigida
OPS	OPS-18.5	O CSP deve consultar os registos online publicados pelos seus fornecedores e prestadores subcontratados pelo menos diariamente, e atualizar de acordo o seu próprio registo online
OPS	OPS-19.2	O CSP deve realizar os testes definidos no OPS-18.1 pelo menos uma vez por mês
OPS	OPS-19.3	A CSP deverá realizar testes de penetração realizados por pessoal interno qualificado ou prestadores de serviços externos, de acordo com uma metodologia de teste documentada e incluir no seu âmbito os componentes do sistema relevantes para a prestação do serviço cloud sob a responsabilidade do CSP, como identificado numa análise de risco
OPS	OPS-19.4	O CSP deve analisar os resultados do teste de penetração e tratar cada vulnerabilidade identificada de acordo com as políticas e procedimentos definidos (cf. OPS-18).
OPS	OPS-20.2	O CSP deve organizar uma revisão trimestral dos resultados da avaliação definida no OPS-20.1 por departamentos responsáveis de forma a iniciar ações de melhoria contínua e verificar sua eficácia
IAM	IAM-01.3	O CSP deve basear a sua política de controlo de acessos em critérios de controlos de acesso baseados na função exercida (role-based).
IAM	IAM-02.2	O CSP deve documentar, comunicar e disponibilizar políticas de gestão de contas de utilizadores sob a responsabilidade do CSP, de acordo com o ISP-02 e estendendo as políticas definidas em IAM-02.1, nas quais pelo menos os seguintes aspetos são descritos: Segregação de funções entre gestão, aprovação e atribuição de contas de utilizador; Revisão regular de contas de utilizador atribuídas e respetivos direitos de acesso; Bloquear e revogar contas em caso de inatividade ou potencial comprometimento da conta; Requisitos para a aprovação e documentação da gestão de contas de utilizadores
IAM	IAM-02.3	O CSP deve documentar, comunicar e disponibilizar políticas de gestão de contas de utilizadores sob a responsabilidade dos CSCs, de acordo com o ISP-02 e estendendo as políticas definidas em IAM-02.1, nas quais pelo menos os seguintes aspetos são descritos: Mecanismos de controlo de acessos disponíveis para CSCs Parâmetros de controlo de acesso que o CSC tem permissão para configurar
IAM	IAM-02.7	O CSP deve providenciar aos CSCs um portal de auto-atendimento/self-service com o qual eles podem gerir as contas de utilizador de forma independente para todos os utilizadores sob a sua responsabilidade.
IAM	IAM-03.2	O mecanismo automatizado no IAM-03.1 deve bloquear contas de utilizador nominais sob a responsabilidade do CSP após dois (2) meses de inatividade.
IAM	IAM-03.4	Os limites de tentativas de autenticação usados no mecanismo IAM-03.3 para contas de utilizador sob a responsabilidade do CSP devem ser baseados nos riscos das contas, direitos de acesso associados e mecanismos de autenticação
IAM	IAM-03.5	O CSP deve documentar um processo para monitorizar credenciais roubadas e comprometidas e bloquear qualquer conta pendente para a qual um problema seja identificado, enquanto se aguarda uma revisão por uma pessoa autorizada
IAM	IAM-03.6	O CSP deve implementar o processo do IAM-03.5 em todas as contas de utilizador sob a sua responsabilidade às quais são atribuídos direitos de acesso privilegiado
IAM	IAM-03.8	A aprovação do pessoal autorizado ou dos componentes do sistema é necessária para desbloquear contas bloqueadas automaticamente
IAM	IAM-03.9	O CSP deve definir e implementar um mecanismo automatizado para revogar as contas de utilizador que tenham sido bloqueadas por outros mecanismos automáticos depois de um certo período de tempo
IAM	IAM-03.10	O mecanismo automatizado de IAM-03.9 deve revogar contas de utilizador sob a responsabilidade do CSP depois elas terem sido bloqueadas por seis (6) meses
IAM	IAM-04.3	O procedimento de atualização ou revogação de direitos de acesso definido em IAM-04.2 deve ser executado dentro de 48 horas da mudança de função para direitos de acesso privilegiado e em 14 dias para outros direitos de acesso.
IAM	IAM-04.7	O CSP deve oferecer aos CSCs um auto-atendimento/self-service com o qual eles podem gerir de forma independente os direitos de acesso para todas as contas de utilizador sob a sua responsabilidade
IAM	IAM-05.2	A revisão definida no IAM-05.1 deve ser realizada por pessoas autorizadas sob a responsabilidade de um órgão autorizado que aprovou o acesso às políticas de direitos.
IAM	IAM-05.3	O CSP trata desvios identificados em tempo útil, no máximo 7 dias após sua deteção, revogando ou atualizando os direitos de acesso de forma adequada.
IAM	IAM-05.4	O CSP deve fornecer aos CSCs uma ferramenta que facilite a revisão dos direitos de acesso das contas de utilizador sob a sua responsabilidade
IAM	IAM-06.1	Os direitos de acesso privilegiado devem ser personalizados, limitados no tempo de acordo com uma avaliação de risco e atribuídos consoante necessário para a execução das tarefas (princípio da necessidade de saber)
IAM	IAM-06.2	Atividades de utilizadores com direitos de acesso privilegiado devem ser registadas- (logs) de modo a se detetar qualquer uso indevido de acesso ou função privilegiada em casos suspeitos, e as informações registadas (logs) devem ser monitorizadas automaticamente para eventos definidos que podem indicar uso indevido

IAM	IAM-06.3	O CSP deve documentar e implementar um procedimento que, ao detetar um possível uso indevido pela monitorização definida em IAM-06.2, informe o responsável para que possa ser avaliado prontamente se o uso indevido ocorreu e serem tomadas as medidas correspondentes.
IAM	IAM-06.7	O CSP deve requerer autenticação forte para aceder as interfaces de administração usadas pelo CSP
IAM	IAM-07.2	O acesso a todos os ambientes do CSP devem ser autenticado, incluindo ambientes de não produção
IAM	IAM-07.5	Num ambiente, a autenticação do utilizador deve ser realizada através de senhas (passwords), certificados assinados digitalmente ou procedimentos que atinjam pelo menos um nível equivalente de segurança
IAM	IAM-07.6	Para acesso a contas partilhadas não nominais, o CSP deve implementar medidas que exijam que os utilizadores sejam autenticados com a sua conta nominal antes de poderem aceder a essas contas técnicas
IAM	IAM-07.8	O CSP deve oferecer métodos de autenticação forte para o CSC usar nas contas sob sua responsabilidade
IAM	IAM-08.2	As regras e recomendações do CSP definidas em IAM-08.1 devem abordar pelo menos os seguintes aspetos: Recomendações sobre gestores de senhas; Recomendações para abordar especificamente ataques clássicos, incluindo *phishing*, ataques sociais e *whaling*
IAM	IAM-08.6	Ao criar credenciais, a conformidade com as especificações deve ser aplicada automaticamente, tanto quanto tecnicamente possível
IAM	IAM-08.7	Quando uma credencial associada a uma conta nominal é alterada ou renovada, a pessoa associada a essa conta deve ser notificada
IAM	IAM-08.8	Qualquer senha comunicada a um utilizador por e-mail, mensagem ou similar deverá ser alterada pelo utilizador após a sua primeira utilização, e sua validade não deverá exceder 14 dias após a comunicação ao utilizador
IAM	IAM-08.9	O CSP deve disponibilizar ao CSC as regras e recomendações que devem ou podem ser aplicadas aos utilizadores sob a sua responsabilidade, e fornecer ao CSC as ferramentas para gerir e fazer cumprir essas regras
IAM	IAM-09.2	O CSP deve projetar, desenvolver, configurar e implementar o sistema de informação que presta o serviço cloud para incluir uma segmentação entre a infraestrutura técnica e o equipamento necessário para a administração do serviço cloud e os ativos TIC que aloja
IAM	IAM-09.5	O CSP deve informar de forma atempada o CSC sempre que os colaboradores internos ou externos do CSP acedem de forma não-criptografada aos dados processados, armazenados ou transmitidos do cliente do serviço cloud sem o prévio consentimento do CSC, incluindo pelo menos: Causa, tempo, duração, tipo e âmbito do acesso; Detalhes suficientes para permitir que especialistas do CSC avaliem os riscos do acesso.
IAM	IAM-09.7	Se o CSP oferecer aos seus CSCs interfaces para administradores e para utilizadores finais, essas interfaces devem ser separadas
CKM	CKM-01.2	As políticas e procedimentos de criptografia devem incluir disposições para o uso de criptografia baseadas no risco alinhadas com os esquemas de classificação de dados e considerando os canais de comunicação, tipo, robustez e qualidade da criptografia
CKM	CKM-01.3	Os procedimentos fortes de criptografia e protocolos de redes seguros mencionados nas políticas e procedimentos de criptografia devem corresponder aos do estado-da-arte
CKM	CKM-03.2	As chaves privadas e secretas utilizadas para criptografia devem ser conhecidas apenas para o cliente cloud em conformidade com as obrigações e requisitos legais e regulamentares aplicáveis, com a possibilidade de exceções
CKM	CKM-03.3	Os procedimentos para o uso de chaves privadas e secretas, incluindo um procedimento específico para quaisquer exceções, devem ser acordados contratualmente com o cliente cloud
CKM	CKM-04.2	Para o seguro de armazenamento de chaves, a chave de gestão do sistema deve ser separada dos níveis aplicacionais e de middleware
CKM	CKM-04.4	Se forem usadas chaves pré-partilhadas, as disposições específicas relacionadas com o uso seguro deste procedimento devem ser especificadas separadamente.
CS	CS-01.2	As garantias técnicas em CS-01.1 devem ser baseadas nos resultados de uma análise de risco realizada de acordo com RM-01.
CS	CS-01.3	O CSP deve carregar num sistema SIEM (Sistema de gestão e correlação de eventos de Segurança de Informação), todos os dados das garantias técnicas implementadas para que as contramedidas automáticas sobre eventos correlacionados sejam iniciadas
CS	CS-03.5	O CSP deve rever pelo menos anualmente o desenho, implementação e configuração realizada para monitorizar as conexões de uma forma orientada para o risco, no que diz respeito aos requisitos de segurança definidos
CS	CS-03.6	O CSP deve avaliar os riscos das vulnerabilidades identificadas de acordo com o procedimento de gestão de risco (cf. RM-01) e as medidas de acompanhamento devem ser definidas e rastreadas (cf.OPS-17)
CS	CS-03.7	O CSP deve proteger todos os registos (logs) do SIEM para evitar adulteração
CS	CS-04.2	Os gateways de segurança devem permitir apenas conexões identificadas legítimas numa matriz de fluxos autorizados
CS	CS-04.3	A autorização de acesso ao sistema para acesso em múltiplas redes (cross-network) deve ser baseada numa avaliação de segurança com base nos requisitos dos clientes cloud.
CS	CS-07.3	No âmbito do inventário de ativos (cf. AM-01), a documentação deve incluir os equipamentos que fornecem funções de segurança e os servidores que alojam ou fornecem funções sensíveis.
CS	CS-07.4	O CSP deve realizar uma revisão completa da documentação da topologia de rede pelo menos uma vez por ano
CS	CS-08.3	O CSP deve garantir que a configuração de redes corresponde ao definido nas políticas de segurança de rede, independentemente dos meios utilizados para a criação da configuração
CS	CS-09.2	A política e os procedimentos devem incluir referências para a classificação de ativos (cf.AM-05)
PI	PI-02.2	As definições do PI-02.1 devem basear-se nas necessidades dos especialistas de potenciais clientes que avaliam a adequação do serviço cloud relativo a uma dependência sobre o CSP, assim como nos requisitos legais e regulamentares.
PI	PI-03.3	Os procedimentos de eliminação de dados do cliente cloud devem impedir a recuperação por meios forenses

PI	PI-03.4	O CSP deve documentar a eliminação dos dados do cliente, incluindo metadados e dados armazenados nos backups, de forma a que cliente cloud consiga rastrear a eliminação dos seus dados
PI	PI-03.5	No fim do contrato, o CSP deve excluir os dados técnicos relativos ao cliente
CCM	CCM-01.2	As políticas e procedimentos de gestão de alterações devem contemplar pelo menos os seguintes aspetos: Critérios para avaliação de risco, categorização e priorização de alterações e requisitos relacionados com o tipo e âmbito dos testes a serem realizados, e as aprovações necessárias; Requisitos para o desempenho e documentação de testes; Requisitos para segregação de funções durante o planeamento, testes e implementação (disponibilização) de alterações; Requisitos para a informação adequada dos clientes cloud sobre o tipo e âmbito das alterações, bem como as obrigações resultantes de acordos de cooperação e os acordos contratuais; Requisitos para a documentação de alterações no sistema e documentação operacional e de utilizador; e Requisitos para a implementação e documentação de alterações de urgência que devem cumprir com o mesmo nível de segurança que alterações normais.
CCM	CCM-02.2	O CSP deve basear a decisão de classificação e priorização numa avaliação de risco realizada de acordo com RM-01 no que diz respeito aos efeitos potenciais nos componentes do sistema em questão
CCM	CCM-03.2	O tipo e âmbito dos testes devem corresponder à avaliação de risco
CCM	CCM-03.3	Os testes devem ser realizados por colaboradores devidamente qualificados ou por procedimentos de teste automatizados que estejam conformes o estado da arte
CCM	CCM-03.4	Em conformidade com requisitos contratuais, o CSP deve envolver os CSCs para os testes.
CCM	CCM-03.5	O CSP deve obter primeiro a aprovação do CSC e anonimizar os dados do cliente antes de serem usados para testes. Além disso, deve garantir a confidencialidade dos dados durante o todo processo
CCM	CCM-03.6	O CSP deve determinar a severidade dos erros e vulnerabilidades identificadas nos testes que são relevantes para a decisão de implementação, de acordo com os critérios definidos, e deve iniciar ações para correção ou mitigação em tempo útil
CCM	CCM-04.2	O CSP deve envolver os CSCs no processo de aprovação de acordo com os requisitos contratuais
DEV	DEV-01.3	As políticas e procedimentos para desenvolvimento seguro devem ser baseadas em normas, referenciais e métodos reconhecidos em relação aos seguintes aspetos: Segurança no Desenvolvimento de Software (Requisitos, Design, Implementação, Teste e Verificação); Segurança na implementação de software (incluindo em entregas contínuas); Segurança na operação (reação às falhas e vulnerabilidades identificadas); e Referenciais e práticas de desenvolvimento de código seguros (evitando a introdução de vulnerabilidades no código).
DEV	DEV-01.4	As políticas e procedimentos para o desenvolvimento devem incluir medidas para a aplicação de normas, referenciais e diretrizes especificadas, incluindo ferramentas automatizadas
DEV	DEV-02.2	O CSP deve documentar e implementar políticas para o uso de software de terceiros e de código aberto
DEV	DEV-02.3	O CSP deve disponibilizar a sua lista de dependências aos clientes, mediante solicitação
DEV	DEV-03.3	O CSP deve implementar ambientes de desenvolvimento e de teste seguros de forma a ser possível gerir todo o ciclo de desenvolvimento do sistema de informação do serviço cloud
DEV	DEV-03.4	O CSP deve considerar os ambientes de desenvolvimento e teste ao realizar a avaliação de risco
DEV	DEV-03.5	O CSP deve incluir recursos de desenvolvimento como parte do backup de política
DEV	DEV-05.2	A documentação de projeto para características de segurança deve incluir uma especificação das entradas e saídas esperadas e possíveis erros, bem como uma análise de segurança da adequação e eficácia planeada para o recurso
DEV	DEV-05.3	Os testes a características de segurança devem contemplar todas as entradas especificadas e todos os resultados especificados, incluindo todas as condições de erro especificadas.
DEV	DEV-05.4	A documentação dos testes para características de segurança deve incluir pelo menos uma descrição do teste, as condições iniciais, o resultado esperado e as instruções para a execução do teste.
DEV	DEV-06.3	Os procedimentos devem incluir as seguintes atividades, dependendo da avaliação de risco: Teste estático de segurança de aplicações; Teste dinâmico de segurança de aplicações; Revisão de Código por especialistas; e Obtenção de informações sobre vulnerabilidades confirmadas em bibliotecas de software fornecidas por terceiros e utilizados no seu próprio serviço cloud.
DEV	DEV-06.5	O CSP deve avaliar a severidade das vulnerabilidades identificadas de acordo com os critérios definidos no OPS-17 e devem ser tomadas medidas para correção ou mitigação de forma imediata
DEV	DEV-07.2	Antes da subcontratação do desenvolvimento do serviço cloud ou componentes dos mesmos, o CSP devem realizar uma avaliação de risco de acordo com a RM-01, considerando, pelo menos, os seguintes aspetos: Gestão do código fonte pelo subcontratado; Procedimentos de recursos humanos implementados pelo subcontratado; e Acessos necessários aos ambientes de desenvolvimento, teste e pré-produção do CSP
PM	PM-01.2	As políticas e procedimentos definidos em PM-01.1 devem contemplar, pelo menos, os seguintes aspetos: Requisitos para a avaliação dos riscos decorrentes da contratação de serviços a terceiros; Requisitos para a classificação de terceiros com base na avaliação de risco do CSP; Requisitos de segurança da informação para o tratamento, armazenamento, ou a transmissão de informações por terceiros baseados em referenciais reconhecidos da indústria; Requisitos de sensibilização e treino em segurança da informação para os colaboradores; Requisitos legais e regulamentares aplicáveis; Requisitos para tratamento de vulnerabilidades, incidentes de segurança e mau funcionamento; Especificações para acordos contratuais destes requisitos;

		Especificações para a monitorização destes requisitos; e Especificações para aplicação destes requisitos, de igual forma, a prestadores de serviços terceiros, na medida em que os serviços prestados por estes também contribuem para a prestação do serviço cloud.
PM	PM-02.2	A avaliação de risco deve incluir a identificação, análise, avaliação, tratamento e documentação dos riscos relativos aos seguintes aspetos: Requisitos de Proteção em relação a confidencialidade, integridade, disponibilidade, e autenticidade das informações tratadas, armazenadas, ou transmitidas pela terceira parte; Impacto de uma violação das proteções da prestação do serviço cloud; A dependência do CSP sobre o prestador de serviço ou fornecedor para o âmbito, complexidade, e singularidade do serviço adquirido, incluindo considerações de possíveis alternativas.
PM	PM-03.2	O diretório deve conter as seguintes informações: Nome da empresa; Endereço; Locais de tratamento e armazenamento de dados; Contacto da pessoa responsável pelo prestador/fornecedor de serviços; Contacto da pessoa responsável pela prestação de serviço cloud; Descrição do serviço; Classificação baseada na avaliação de risco; Início da utilização do serviço; e Prova de conformidade com os requisitos contratualmente acordados
PM	PM-04.2	As atividades de monitorização devem incluir, pelo menos, uma revisão regular às seguintes evidências fornecidas pelos fornecedores no âmbito dos acordos contratuais: Relatórios sobre a qualidade do serviço prestado; certificados de os de gestão de sistemas conformidade com internacionais normas; relatórios de terceiros independentes sobre a adequação e eficácia operacional de seus sistemas de controle interno relacionados ao serviço; e Registros dos terceiros partidos sobre a manipulação de vulnerabilidades, segurança incidentes, e avarias.
PM	PM-04.6	O CSP deve documentar e implementar um processo de revisão e atualização, pelo menos uma vez um ano, de requisitos de não divulgação ou confidencialidade relativos a fornecedores que contribuem para a prestação do serviço
PM	PM-05.2	As estratégias de saída devem estar alinhadas com os planos de continuidade operacional e incluir os seguintes aspetos: Análise dos potenciais custos, impactos, recursos, e tempo da transição de uma compra de serviço para um fornecedor ou prestador de serviço alternativo; Definição e alocação de funções, responsabilidades e recursos suficientes para realizar as atividades de transição; Definição de critérios de sucesso para a transição; Definição de indicadores para o desempenho do serviço de monitorização, que deve iniciar a retirada do serviço, se os resultados não forem aceitáveis.
IM	IM-01.4	O CSP deve informar de forma oportuna e adequada os clientes afetados por incidentes de segurança
IM	IM-01.5	A política de gestão de incidentes deve incluir procedimentos de como os dados de um sistema suspeito podem ser recolhidos de forma conclusiva, como em situações de incidentes de um segurança.
IM	IM-02.2	O CSP deve manter um catálogo que identifique claramente os incidentes de segurança que afetam os dados do cliente e usar esse catálogo para classificar os incidentes
IM	IM-02.3	O mecanismo de classificação de incidentes deve incluir disposições para correlacionar eventos. Além disso, esses eventos correlacionados devem ser avaliados e classificados de acordo com sua criticidade
IM	IM-03.3	O CSP deve reportar continuamente o estado de um incidente de segurança aos clientes afetados até que esta seja resolvido e seja aplicada e documentada uma solução, de acordo com os SLAs definidos e acordos contratuais
IM	IM-06.3	O CSP deve definir, implementar e manter um repositório de conhecimento de incidentes de segurança e as medidas tomadas para os resolver, bem como informações relacionadas com os ativos que estes incidentes afetaram, e usar essa informação para enriquecer o catálogo de classificação.
IM	IM-06.4	A inteligência obtida com a gestão de incidentes e existente no repositório de conhecimento, deve ser usada para identificar incidentes recorrentes ou potenciais incidentes significativos, e para determinar a necessidade de garantias avançadas e a sua implementação
IM	IM-07.2	Os documentos e provas devem ser arquivados de uma forma que possa ser utilizada como prova em tribunal
IM	IM-07.3	Quando o CSP requer experiência adicional para preservar as evidências e proteger a cadeia de custódia de um incidente de segurança, o CSP deve contratar um prestador de serviços qualificado em resposta a incidentes
BC	BC-01.2	O CSP deve nomear (um membro da) gestão de topo como o responsável do processo de continuidade de negócio e gestão de crises. Este é responsável por estabelecer o processo dentro na organização através de uma estratégia, bem como garantir o cumprimento das diretrizes e disponibilidade de recursos suficientes para um processo eficaz
BC	BC-01.3	O responsável pelo processo de gestão de continuidade de negócio e contingência deve garantir a disponibilidade de recursos suficientes para um processo eficaz
BC	BC-02.2	As políticas e procedimentos de análise de impacto de negócio devem considerar, pelo menos, os seguintes aspetos: Cenários possíveis com base numa análise de risco; Identificação de produtos e serviços críticos; Identificação de dependências, incluindo processos (incluindo recursos necessários), aplicações, parceiros de negócios e terceiros; Identificação de ameaças a produtos e serviços críticos; Identificação de efeitos resultantes de avarias planeadas e não planeadas e alterações ao longo do tempo; Determinação da duração máxima de avarias; Identificação de prioridades de restauração;

		Determinação do tempo para a reposição de produtos e serviços críticos dentro do período de tempo máximo aceitável (RTO); Determinação do tempo para o período máximo razoável durante o qual os dados podem ser perdidos e não recuperados (RPO); e Estimativa dos recursos necessários para a reposição.
BC	BC-02.3	A análise de impacto do negócio resultante das políticas e procedimentos devem ser revistos em intervalos regulares, pelo menos uma vez por ano, ou depois de alterações significativas organizacionais ou no ambiente.
BC	BC-03.2	O plano de continuidade de negócio e planos de contingência devem ser baseados em referenciais aceites pela indústria e devem documentar quais estão a ser usados.
BC	BC-03.3	O plano de continuidade de negócio e os planos de contingência devem contemplar pelo menos os seguintes aspetos: Objetivo e âmbito definidos, incluindo processos de negócios e dependências relevantes; Acessibilidade e compreensibilidade dos planos para as pessoas agirem em conformidade; Responsabilidade de existir, pelo menos, uma pessoa designada para rever, atualizar e aprovar; Definição de canais de comunicação, papeis e responsabilidades, incluindo a notificação do cliente; Procedimentos de recuperação, soluções provisórias manuais e informações de referência (levando em consideração a priorização na recuperação de componentes e serviços da infraestrutura cloud e alinhamento com os clientes); Métodos para colocar os planos em prática; Melhoria contínua de processos; e Interfaces para gestão de incidentes de segurança.
BC	BC-03.4	O plano de continuidade de negócio deve ser revisto em intervalos regulares, pelo menos uma vez um ano, ou após alterações significativas relacionadas com o ambiente ou organizacionais.
BC	BC-04.1	A análise de impacto de negócio, plano de continuidade de negócio e planos de contingência devem ser testados em intervalos regulares (pelo menos uma vez por ano) ou após uma atualização
BC	BC-04.2	Os testes devem ser documentados e os resultados considerados para atualizar o plano de continuidade de negócio e definir futuras medidas de continuidade operacional
BC	BC-04.3	Os testes devem envolver CSCs e terceiros relevantes, tais como prestadores de serviços e fornecedores externos
CO	CO-01.2	O CSP deve documentar e implementar procedimentos para estar em conformidade com as exigências contratuais
CO	CO-02.2	O CSP deve documentar e implementar um programa de auditoria ao longo de três anos que define o âmbito e a frequência das auditorias, de acordo com a gestão de alterações, políticas, e os resultados da avaliação de risco
CO	CO-03.3	As vulnerabilidades e desvios identificados devem ser sujeitos à avaliação de risco de acordo com o procedimento de gestão de risco (cf. RM-01) e medidas de acompanhamento devem ser definidas e rastreadas (cf. OPS-17).
CO	CO-03.7	O CSP deve informar os CSCs que operem um serviço cloud certificado de acordo com EUCS de não conformidades em relação aos requisitos de EUCS
CO	CO-04.2	Estas informações devem ser incluídas na revisão da gestão do sistema de controlo interno que é realizada, pelo menos, uma vez por ano
DOC	DOC-01.2	As orientações e recomendações para o uso seguro do serviço cloud devem contemplar, pelo menos, os seguintes aspetos, quando aplicáveis: Instruções para configuração segura; Fontes de informação sobre vulnerabilidades conhecidas e mecanismos de atualização; Tratamento de erros e mecanismos de registo (logging); Mecanismos de autenticação; Conceito de funções e direitos, incluindo combinações que resultam num risco elevado; Serviços e funções de administração do serviço cloud por utilizadores privilegiados, e Controlos Complementares do Cliente (CCCs).
DOC	DOC-01.4	O CSP deve descrever na documentação do utilizador todos os riscos partilhados com o cliente
DOC	DOC-02.2	O registo online de vulnerabilidades também deve incluir vulnerabilidades conhecidas que afetam os ativos fornecidos pelo CSP que os clientes cloud devem instalar, fornecer ou operar sob a responsabilidade do cliente
DOC	DOC-02.3	A apresentação das vulnerabilidades deve seguir um sistema de classificação aceite pela indústria para a descrição das vulnerabilidades.
DOC	DOC-02.4	A informação contida no registo online deve incluir informações suficientes para formar uma base adequada para a avaliação de risco e possíveis medidas de acompanhamento de utilizadores cloud.
DOC	DOC-02.5	Para cada vulnerabilidade, o registo online deve indicar se as atualizações de software estão disponíveis, quando serão lançadas e se serão implementadas pelo CSP, o CSC ou ambos
DOC	DOC-03.3	O CSP deve fornecer informações sobre: Os locais de administração e supervisão podem ser utilizados no serviço cloud; Os locais para os quais quaisquer dados de cliente cloud, metadados ou dados derivados podem ser transferidos, tratados ou armazenados.
DOC	DOC-04.4	A justificação deve ser baseada numa análise de risco de acordo com RM-01
DOC	DOC-05.4	O CSP deve classificar cada requisito associado aos CCC com o nível de garantia mais baixo EUCS para o qual é exigido
DOC	DOC-06.3	O CSP deve justificar as contribuições num documento complementar
INQ	INQ-03.3	Quando nenhuma limitação dos dados é aplicável, o CSP deve anonimizar ou pseudonimizar os dados para que as agências governamentais só possam atribuí-los aos clientes cloud que estão sujeitos ao pedido de investigação
PSS	PSS-01.2	As informações fornecidas devem ser detalhadas o suficiente para permitir que os utilizadores da cloud verifiquem os seguintes aspetos, na medida em que sejam aplicáveis ao serviço cloud: Os dados, serviços ou funções que são disponibilizados para o utilizador cloud no âmbito do serviço cloud, têm que ser registados de acordo com que acessos feitos por quem e quando (Audit Logs); Falhas durante o processamento de ações automáticas ou manuais; e

		Alterações nos parâmetros de configuração relevantes para a segurança, tratamento de erros e mecanismos de registo (logs), autenticação de utilizadores, autorização de ações, criptografia e segurança de comunicações.
PSS	PSS-01.3	As informações registadas (logs) devem ser protegidas contra o acesso não autorizado, modificações e podem ser eliminadas pelo CSC
PSS	PSS-01.4	Quando o CSC é responsável pela ativação ou tipo e âmbito do registo (logging), o CSP deve fornecer os recursos de registo adequados
PSS	PSS-02.2	O sistema de gestão de sessões deve incluir mecanismos que invalidem uma sessão após ela ter sido detetada como inativa.
PSS	PSS-02.3	Se a inatividade for detetada pela medição do tempo, o intervalo de tempo deve ser configurável pelo CSP ou - se tecnicamente possível - pelo CSC
PSS	PSS-03.3	O CSP deve garantir que a configuração de redes está de acordo com as políticas de segurança de rede, independentemente dos meios utilizados para criar a configuração
PSS	PSS-04.2	O CSP deve garantir os seguintes aspetos se os CSCs operam máquinas virtuais ou containers com o serviço cloud: Se o CSP fornece imagens de máquinas virtuais ou recipientes para o CSC, o CSP adequadamente informar o CSC de que as alterações feitas para a anterior versão
PSS	PSS-05.1	O CSP deve permitir que o CSC especifique os locais (localização / país) do tratamento e armazenamento de dados, incluindo os backups de dados, de acordo com as opções contratualmente disponíveis
PSS	PSS-05.2	Todos os "commits" do CSP sobre locais de tratamento e armazenamento de dados devem ser aplicados pela arquitetura do serviço cloud

(os requisitos a sombreado estão diretamente relacionados com o EUCS)

19. Anexo IV - Requisitos de Segurança com Nível de Garantia Alto

Ref.1	Ref.2	Descrição
OIS	OIS-01.3	O SGSI deve ter uma certificação válida de acordo com a ISO / IEC 27001 ou esquemas nacionais baseados na ISO 27001
OIS	OIS-01.5	A documentação deve incluir pelo menos: Âmbito do SGSI (Secção 4.3 da norma ISO / IEC 27001); Declaração de aplicabilidade (Seção 6.1.3), e Resultados da última revisão da gestão (Seção 9.3).
OIS	OIS-02.4	O CSP deve monitorizar automaticamente a atribuição de responsabilidades e tarefas para garantir que as medidas relacionadas à segregação de funções sejam aplicadas.
OIS	OIS-03.3	O CSP deve manter contato regular com seu CAB e NCCA para se manter informado sobre as ameaças e vulnerabilidades atuais
ISP	ISP-01.4	O CSP deve rever a política global de segurança da informação pelo menos anualmente
ISP	ISP-02.5	Em caso de delegação, os órgãos autorizados devem reportar, pelo menos, anualmente à gestão de topo sobre as políticas de segurança e a sua implementação
ISP	ISP-03.4	As exceções para a política de segurança ou procedimento devem ser aprovadas pela gestão de topo ou pelo órgão autorizado que aprovou a política de segurança ou procedimento
ISP	ISP-03.7	A lista de exceções deve ser monitorizada automaticamente para garantir que a validade das exceções aprovadas não tenha expirado e que todas as análises e aprovações estão atualizadas
RM	RM-02.4	O CSP deve monitorizar a evolução dos fatores de risco e rever os resultados da avaliação de risco em conformidade
HR	HR-02.4	A competência e integridade dos colaboradores internos e externos do CSP devem ser revistas anualmente para os colaboradores com cargos em níveis elevados de classificação de risco, começando no nível que for ser definido na política de recursos humanos.
HR	HR-03.5	A verificação do reconhecimento definido em HR-03.4 deve ser monitorizada automaticamente em processos e sistemas automatizados utilizados para conceder direitos de acesso aos colaboradores.
HR	HR-04.7	O CSP deve monitorizar automaticamente a conclusão do programa de sensibilização e treino de segurança
HR	HR-04.9	O CSP deve medir e avaliar de forma orientada ao público-alvo os resultados de aprendizagem alcançados através do programa de sensibilização e treino de segurança. As medições devem abranger aspetos quantitativos e qualitativos, e os resultados devem ser usados para melhorar programa de sensibilização e treino de segurança.
HR	HR-05.4	O CSP deve monitorizar automaticamente a aplicação do procedimento mencionado no HR- 05.2
HR	HR-06.7	O CSP deve monitorizar automaticamente a confirmação de acordos de não divulgação ou confidencialidade por colaboradores internos, prestadores de serviços externos e fornecedores.
AM	AM-01.5	As informações sobre os ativos devem ser consideradas por aplicações de monitorização para identificar o impacto nos serviços cloud e funções em caso de eventos que possam levar a uma violação dos objetivos de proteção, e para apoiar as informações fornecidas aos clientes cloud afetados de acordo com os acordos contratuais
AM	AM-01.6	O CSP deve monitorizar automaticamente o seu inventário de ativos para garantir que está atualizado
AM	AM-02.3	Quando dispositivos removíveis são usados na infraestrutura técnica ou para tarefas de administração TIC, devem ser dedicados a um único uso
AM	AM-03.6	A aprovação do comissionamento e desmantelamento do hardware deve ser documentada digitalmente e monitorizada automaticamente.
AM	AM-04.3	O CSP deve gerir centralmente os ativos sob custódia de colaboradores internos e externos, incluindo, pelo menos, software, dados e distribuição de políticas, bem como a desativação remota, apagar ou bloquear, conforme disponível no ativo.
AM	AM-04.4	A verificação do compromisso definido na AM-04.1 deve ser monitorizado automaticamente
PS	PS-01-3	O CSP deve definir no mínimo, uma área privada adicional que pode contemplar as atividades de desenvolvimento e administração, supervisão e estações de trabalho de operações
PS	PS-01.4	O CSP deve garantir que não existe acesso direto entre uma área pública e uma área sensível
PS	PS-01.5	O CSP deve assegurar que todas as áreas de entrega, de carga e outros pontos através dos quais pessoas não autorizadas podem entrar nas instalações sem serem acompanhadas, fazem parte da área pública
PS	PS-02.6	A política de controlo de acessos deve descrever os intervalos de tempo e as condições de acesso a cada área, de acordo com o perfil dos utilizadores
PS	PS-02.10	O registo dos acessos deve ser monitorizado automaticamente para garantir o cumprimento do PS-02.9
PS	PS-03.3	O CSP deve definir um mapeamento entre as atividades e as zonas indicando quais atividades que podem/não devem/devem ser realizadas em cada área de segurança
PS	PS-03.4	O CSP deve definir um mapeamento entre ativos e as zonas indicando quais ativos que podem/não devem/devem ser usados em cada área de segurança
PS	PS-04.4	O procedimento mencionado no PS-04.3 deve incluir uma validação formal pela gestão de topo do CSP ou pelo órgão autorizado que validou este procedimento
PS	PS-04.5	O CSP deve estabelecer um esquema de cablagem e mantê-lo atualizado
PS	PS-04.6	O CSP deve assegurar que os acordos de manutenção para o equipamento utilizado no alojamento do serviço cloud contemplem a instalação de atualizações de segurança regulares sobre este equipamento
PS	PS-04.7	As políticas e procedimentos em PS-04.1 devem incluir medidas para garantir que as condições de instalação, manutenção e serviço do equipamento técnico relacionado (por exemplo, energia elétrica, ar condicionado, proteção contra incêndios) sejam compatíveis com os requisitos de disponibilidade e segurança do serviço cloud

PS	PS-04.8	O CSP deve assegurar que um equipamento contendo um dispositivo com os dados do cliente pode ser devolvido a uma terceira parte apenas se os dados armazenados dos clientes estiverem criptografados em conformidade com CKM-03 ou tenham sido destruídos previamente usando um mecanismo de eliminação seguro
PS	PS-05.3	Os requisitos de segurança definidos no PS-05.1 para datacenters devem incluir restrições de tempo para operação autossuficiente no caso de eventos excecionais e tempo de inatividade máximo tolerável
PS	PS-05.4	Os requisitos de segurança definidos no PS-05.1 para datacenters devem incluir testes de equipamentos de proteção e deteção física, a serem realizados pelo menos anualmente
OPS	OPS-01.3	As projeções de capacidade devem ser consideradas de acordo com os níveis de serviço para o planeamento e preparação do provisionamento
OPS	OPS-02.2	O CSP deve disponibilizar ao cliente cloud as informações relevantes sobre capacidade e disponibilidade de um portal de auto-atendimento (self-service)
OPS	OPS-02.3	O provisionamento e desprovisionamento de serviços cloud devem ser monitorizados automaticamente para garantir o cumprimento da OPS-02.1
OPS	OPS-04.3	As políticas e instruções relacionadas com malware devem incluir as medidas técnicas tomadas para uma configuração segurança, proteção contra malware e monitorização das interfaces de administração (tanto o autoatendimento/self-service do cliente como a administração do CSP)
OPS	OPS-04.4	O CSP deve atualizar os produtos anti-malware na maior frequência que os fornecedores atualmente ofereçam
OPS	OPS-05.3	O CSP deve monitorizar automaticamente os sistemas cobertos pela proteção contra malware e a configuração dos mecanismos correspondentes para garantir o cumprimento do OPS-05.1
OPS	OPS-05.4	O CSP deve monitorizar automaticamente os scans de antimalware para rastrear o malware detetado ou irregularidades
OPS	OPS-07.2	O CSP deverá disponibilizar aos seus clientes um portal de auto-atendimento/self-service para monitorização automática dos backups dos seus dados e garantir o cumprimento da OPS-07.1
OPS	OPS-07.3	O CSP deve monitorizar automaticamente os seus backups de dados para garantir o cumprimento da OPS-07.1
OPS	OPS-08.4	O CSP deve informar os CSCs, a seu pedido, dos resultados dos testes de recuperação
OPS	OPS-08.5	Os testes de recuperação devem estar incluídos na gestão de continuidade de negócio do CSP
OPS	OPS-09.5	Quando os dados de backup são transmitidos para um local remoto por meio de uma rede, o CSP deve monitorizar automaticamente a sua transmissão para garantir o cumprimento da OPS-09.1
OPS	OPS-11.4	Os dados derivados, incluindo dados de registo (logs), devem ser tidos em consideração nas avaliações de conformidade regulamentar.
OPS	OPS-12.4	O CSP deve monitorizar automaticamente que a deteção de eventos é eficaz sobre a lista de ativos críticos no cumprimento da OPS-12.1
OPS	OPS-13.6	O CSP deve fornecer aos CSCs, mediante solicitação, acesso ao registo específico do cliente através de uma API. O registo deve estar em conformidade com os requisitos de proteção do CSP, incluindo a separação lógica ou física do registo e dos dados do cliente
OPS	OPS-13.7	O CSP deve monitorizar automaticamente a agregação e eliminação de dados de registo e monitorização para cumprir OPS-13.2
OPS	OPS-14.3	No contexto de uma investigação de um incidente relativo a um CSC, o CSP deve ter a capacidade de fornecer ao CSC os registos (logs) relacionados com o seu serviço cloud
OPS	OPS-16.2	O CSP deve projetar os componentes do sistema de registo e monitorização de forma a que a funcionalidade total é não comprometida se componentes individuais falharem
OPS	OPS-18.6	O CSP deve equipar, com mecanismos de atualização automática, os ativos fornecidos pelo CSP que os CSCs têm que instalar ou operar sob sua própria responsabilidade, para facilitar a implementação de patches e atualizações após a aprovação inicial do CSC
OPS	OPS-19.5	Os testes são realizados seguindo um programa de trabalho plurianual, revisto anualmente, que contemple os componentes do sistema e controlos de segurança de acordo com a evolução do serviço cloud e o panorama de ameaças.
OPS	OPS-19.6	Alguns dos testes de penetração realizados a cada ano devem ser realizados por prestadores de serviços externos
OPS	OPS-19.7	O CSP deve realizar uma análise das causas raiz das vulnerabilidades encontradas através de testes de penetração para avaliar em que medida vulnerabilidades semelhantes podem estar presentes no sistema cloud
OPS	OPS-19.8	O CSP deve correlacionar as possíveis explorações de vulnerabilidades encontradas com incidentes anteriores para identificar se a vulnerabilidade pode ter sido explorada antes da sua descoberta
OPS	OPS-21.3	O CSP deve monitorizar automaticamente os componentes do serviço sob sua responsabilidade em conformidade com as especificações de proteção
IAM	IAM-02.8	O CSP deve ser capaz de fornecer, para uma determinada conta de utilizador, se ela recai sob a responsabilidade do CSP ou do CSC, assim como a lista de direitos de acesso concedidos a essa conta.
IAM	IAM-03.7	O CSP deve implementar o processo do IAM-03.5 em todas as contas de utilizador sob a sua responsabilidade
IAM	IAM-03.11	O CSP deve monitorizar automaticamente os mecanismos automatizados implementados para garantir sua conformidade com IAM-03
IAM	IAM-03.12	O CSP deve monitorizar automaticamente as condições ambientais de tentativas de autenticação e sinalizar eventos suspeitos para o utilizador correspondente ou para pessoas autorizadas
IAM	IAM-04.4	O CSP deve documentar um procedimento para fornecer, para um determinado recurso sujeito ao controlo de acessos, a lista de todas as contas de utilizador que têm acesso a ele e para cada conta, a lista de direitos de acesso atualmente concedidos, sejam elas da responsabilidade do CSP ou de um CSC.
IAM	IAM-04.5	O CSP deve documentar a incompatibilidade entre os direitos de acesso e aplicar essas incompatibilidades quando os direitos de acesso são concedidos ou atualizados numa conta de utilizador
IAM	IAM-04.6	Os procedimentos de gestão de direitos de acesso devem seguir uma abordagem dinâmica
IAM	IAM-05.5	O CSP deve realizar a revisão definida em IAM-05.1 pelo menos a cada seis (6) meses

IAM	IAM-06.5	O CSP deve rever a cada três (3) meses a lista de colaboradores que são responsáveis por uma conta técnica dentro de seu âmbito de responsabilidade
IAM	IAM-06.6	O CSP deve manter atualizado um inventário das contas de utilizador que têm direitos de acesso privilegiados sob a sua responsabilidade
IAM	IAM-06.8	O CSP deve requerer autenticação forte para aceder às interfaces de administração oferecidas ao CSC
IAM	IAM-07.3	O acesso a ambientes de produção do CSP devem ter forte autenticação
IAM	IAM-07.4	O acesso a todos os ambientes do CSP contendo dados do CSC devem ter autenticação forte
IAM	IAM-08.3	O CSP deve exigir que os utilizadores a quem forneça credenciais de autenticação assinem uma declaração na qual garantam que tratam a autenticação pessoal (ou partilhada) de forma confidencial e a mantêm exclusivamente para si próprios
IAM	IAM-09.3	O CSP deve separar as interfaces de administração disponíveis para os CSCs dos disponibilizados aos seus colaboradores internos e externos, e em particular: As contas de administração sob a responsabilidade do CSP devem ser geridas através de ferramentas e diretórios que são separados dos utilizados para a gestão de contas de utilizadores sob a responsabilidade das CSCs; As interfaces de administração disponíveis para o CSCs não devem permitir qualquer conexão através de contas sob a responsabilidade do CSP; As interfaces de administração utilizadas pelo CSP não devem ser acessíveis através de redes públicas e como tal não devem permitir qualquer conexão de contas sob a responsabilidade do CSC.
IAM	IAM-09.6	O CSP deve exigir o consentimento prévio de um CSC antes de qualquer acesso de forma não criptografada aos dados processados, armazenados ou transmitidos do cliente do serviço cloud, fornecendo informações significativas conforme definido em IAM-09.5.
CKM	CKM-02.2	O CSP deve definir e implementar mecanismos de criptografia fortes para a transmissão de todos os dados em redes públicas
CKM	CKM-03.4	As chaves privadas e secretas usadas para criptografia devem ser conhecidas exclusivamente, e sem exceções, pelo cliente cloud de acordo com as obrigações e requisitos legais e regulamentares aplicáveis
CKM	CKM-04.3	Para o armazenamento seguro de chaves e outros segredos usados para as tarefas de administração, o CSP deve usar um container, software ou hardware com segurança adequada
CS	CS-01.4	O CSP deve implementar garantias técnicas para garantir que nenhum dispositivo desconhecido (físico ou virtual) se junte à sua rede (física ou virtual)
CS	CS-01.5	O CSP deve usar diferentes tecnologias nas suas garantias técnicas para evitar que uma única vulnerabilidade leva para a simultânea violação de várias linhas de defesa
CS	CS-04.4	Cada perímetro de rede deve ser controlado por gateways de segurança redundantes e altamente disponíveis
CS	CS-04.5	O CSP deve monitorizar automaticamente o controlo dos perímetros da rede para garantir o cumprimento do CS-04.1
CS	CS-05.4	Quando as redes de administração não são segregadas fisicamente de outras redes, os fluxos de administração devem ser transmitidos num túnel fortemente criptografado.
CS	CS-05.5	O CSP deve definir e configurar uma firewall de aplicação para proteger as interfaces de administração destinadas aos CSCs e expostas numa rede
CS	CS-06.2	Ao implementar recursos de infraestrutura, a segregação segura deve ser garantida por redes fisicamente separadas ou por VLANs fortemente criptografadas
PI	PI-01.5	O CSP deve permitir que aos seus clientes verificar se as interfaces fornecidas (e sua segurança) são adequadas para os seus requisitos de proteção antes do início da utilização do serviço cloud e cada vez que as interfaces são alteradas
PI	PI-02.3	O CSP deve identificar, pelo menos uma vez por ano, os requisitos legais e regulamentares que podem ser aplicados a estes aspetos e ajusta-los os acordos contratuais em conformidade
CCM	CCM-02.3	Se o risco associado a um planeamento de alterações é elevado, devem ser implementadas medidas de mitigação apropriadas antes de disponibilizar o serviço
CCM	CCM-02.4	Em conformidade com acordos contratuais, o CSP deve enviar aos orgãos autorizados do CSC informações sobre a ocasião, hora, duração, tipo e âmbito da alteração, para que possam realizar a sua própria avaliação de risco antes da alteração ser disponibilizada em ambiente de produção
CCM	COM-02.5	Independentemente de acordos contratuais, o CSP deve informar o CSC de alterações que têm a categoria de risco mais alta com base em sua avaliação de risco, conforme mencionado no CCM-02.3
CCM	CCM-03.7	Os testes realizados antes da implementação de alterações devem incluir testes no serviço executado num ambiente de pré-produção
CCM	CCM-03.8	A CSP deve documentar e implementar um processo que garanta a integridade dos dados de teste utilizados em pré-produção
CCM	CCM-03.9	Antes de implementar alterações num componente do sistema, o CSP deve realizar testes de regressão noutros componentes do serviço cloud que dependem desse componente para verificar a ausência de efeitos indesejáveis
CCM	CCM-03.10	O CSP deve monitorizar automaticamente a definição e execução de testes relativos a uma alteração, bem como a correção ou mitigação de problemas
CCM	CCM-04.3	O CSP deve monitorizar automaticamente as aprovações de alterações implementadas no ambiente de produção para garantir o cumprimento do CCM-04.1
CCM	CCM-05.3	O CSP deve monitorizar automaticamente as alterações no ambiente de produção para garantir o cumprimento do CCM-05.1
CCM	CCM-06.2	Os procedimentos de controlo de versões devem estabelecer as garantias e garantias adequadas para assegurar que a confidencialidade, integridade e disponibilidade dos dados dos clientes cloud não são comprometidas quando os componentes de sistema são restaurados ao seu estado anterior
CCM	CCM-06.3	O CSP deve manter um histórico das versões de software e dos sistemas que são implementados, de forma a ser possivel reconstituir, quando aplicável, num ambiente de teste, um ambiente completo como o que foi

		implementado numa determinada data; o tempo de retenção para esse histórico deve ser, pelo menos, o mesmo que para backups (cf. OPS-06)
DEV	DEV-02.4	Na aquisição para o desenvolvimento de serviço cloud, o CSP deve realizar uma avaliação de risco para cada produto de acordo com RM-01
DEV	DEV-04.3	Quando ambientes não-produtivos são expostos através de redes públicas, os requisitos segurança devem ser equivalentes aos definidos para o ambiente de produção
DEV	DEV-05.5	A documentação dos testes deve incluir uma demonstração da cobertura do código fonte, incluindo a cobertura de ramificações para código crítico em termos de segurança.
DEV	DEV-06.4	As revisões do código devem ser realizadas regularmente por pessoas qualificadas ou através de pessoas contratadas.
DEV	DEV-06.6	Os procedimentos para identificar tais vulnerabilidades também devem incluir revisões de código anuais e testes de penetração de segurança por especialistas, como parte do programa anual definido no OPS-19
DEV	DEV-07.3	O CSP deve documentar e implementar um procedimento que possibilite a supervisão e o controlo da atividade de desenvolvimento subcontratualizada, de forma a garantir que esta atividade de desenvolvimento está em conformidade com a política de desenvolvimento seguro do CSP e exista um nível de segurança do desenvolvimento externo que é equivalente ao de desenvolvimento interno.
DEV	DEV-07.4	colaboradores internos ou externos do CSP devem executar os testes relevantes para a decisão de implementação, quando uma alteração inclui o resultado de desenvolvimento subcontratualizado.
PM	PM-01.3	O CSP deve requerer contratualmente que as organizações de subserviços apresentem relatórios regulares de auditores independentes sobre a adequação do desenho e a eficácia do funcionamento do seu sistema de controlo interno relacionado com os serviços, no que diz respeito aos requisitos da EUCS .
PM	PM-01.4	Os relatórios devem incluir os controlos complementares do prestador de subserviços que são necessários, conjuntamente com os controlos do CSP para atender aos requisitos de EUCS aplicáveis com garantida conformidade
PM	PM-01.5	No caso das organizações fornecedoras não serem capazes de fornecer um relatório de conformidade com o EUCS, o CSP deve reservar-se no direito de, através de pessoas qualificadas, os auditar para avaliar a adequação e eficácia dos controlos internos e complementares relacionados com o serviço
PM	PM-04.7	O CSP deve complementar os procedimentos de verificação da conformidade com monitorizações automáticas, impulsionando procedimentos automatizados relacionados com os seguintes aspetos: Configuração de componentes do sistema; Desempenho e disponibilidade de componentes do sistema; Tempo de resposta a avarias e incidentes de segurança; e Tempo de recuperação (tempo até a conclusão do tratamento de erros).
PM	PM-04.8	O CSP deve monitorizar automaticamente as violações e discrepâncias identificadas, e estas devem ser comunicadas automaticamente para os responsáveis ou componentes do sistema do CSP para realizarem uma avaliação rápida e tomarem as devidas ações
IM	IM-01.6	A política de gestão de incidentes deve incluir planos de análise para incidentes típicos de segurança
IM	IM-01.7	A política de gestão de incidentes deve incluir uma metodologia de avaliação para que recolha de informações que não perca o seu valor probatório em qualquer avaliação legal posterior
IM	IM-01.8	A política de gestão de incidentes deve incluir disposições sobre testes regulares das capacidades de resposta a incidentes, para determinar a eficácia geral dessas capacidades e para identificar potenciais deficiências
IM	IM-02.4	O CSP deve simular a identificação, análise e defesa de incidentes e ataques de segurança pelo menos uma vez por ano, por meio de testes e exercícios
IM	IM-02.5	O CSP deve monitorar o tratamento do incidente para verificar a aplicação das política e procedimentos de gestão de incidentes
IM	IM-03.4	O CSP deve permitir que os clientes aprovem ativamente a solução antes da mesma ser aprovada automaticamente depois de um certo período
IM	IM-07.5	O prestador de serviços deve ter uma equipa integrada de resposta forense / incidentes com pessoas especificamente treinadas em provas de preservação e gestão de cadeia de custódia
BC	BC-04.4	Adicionalmente aos testes, também devem ser levados a cabo exercícios, que devem, entre outras coisas, ser baseados em cenários resultantes de incidentes de segurança que tenham já ocorrido no passado
CO	CO-01.3	O CSP deve fornecer estes procedimentos quando solicitado por um CSC
CO	CO-01.4	O CSP deve documentar e implementar um ativo de monitorização dos requisitos legais, regulamentares e contratuais que afetam o serviço
CO	CO-02.3	O CSP deve conceder aos seus CSCs as informações contratualmente garantidas e definir os seus direitos de auditoria
CO	CO-03.4	As auditorias internas devem ser complementadas por procedimentos para monitorizar automaticamente a conformidade com os requisitos aplicáveis de políticas e instruções
CO	CO-03.5	O CSP deve implementar monitorização automatizada para identificar vulnerabilidades e desvios, que devem ser automaticamente comunicados aos especialistas do CSP para avaliação imediata e respetiva ação
DOC	DOC-01.5	O CSP deve analisar regularmente como os CSCs aplicam as recomendações de segurança e CCCs, e tomar medidas para incentivar a conformidade com base no modelo de responsabilidade partilhada definido
DOC	DOC-02.6	O CSP deve equipar com mecanismos de atualização automática os ativos que fornece que devem ser instalados, fornecidos ou operados por CSCs dentro da sua área de responsabilidade
DOC	DOC-03.4	O CSP deve documentar os locais através dos quais se realizam as operações de suporte para clientes, e deve documentar a lista de operações que podem ser realizadas pelo suporte ao cliente em cada localização
PSS	PSS-01.5	O CSP deve disponibilizar as informações aos CSCs por meio de interfaces documentadas que sejam adequadas para o tratamento posterior dessas informações como parte de seu Sistema de Gestão de Informações e Eventos de Segurança (SIEM).

PSS	PSS-04.3	Uma verificação de integridade deve ser realizada e automaticamente monitorizada para detetar manipulações de imagem e reportadas ao CSC no início e tempo de execução da máquina virtual ou imagens de container

(os requisitos a sombreado estão diretamente relacionados com o EUCS)